

NORMAN®

Kriminalitetsutviklingen på Internett.

- Hva kan vi forvente videre framover?
- Hva gjør antivirusselskapene?

Christophe Birkeland

CTO

Norman

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

NORMAN®

Company Overview

- Founded in 1984 - HQ in Lysaker.
- Direct operations in 7 countries
- Approx 200 employees
(R&D: 55 in Oslo, 25 in India, currently expanding)
- Markets: Consumers, Business, Government, OEM, Industry
- 40.000 Business Customers
- Over 2500 Partners worldwide
- Strong partnerships with key industry leaders



NORMAN®

Overview

- Cyber crime & Threat picture:
 - WHAT
 - WHY
 - WHO
- Advanced Persistent Threat (APT)
- Advices – What can we do ?



What is malware?

Norman Malware Analysis Generation 2

Task Details

Risk level: 9

Received: 2011-11-17 20:57:21

Analyzed: 2011-11-17 20:57:39

Processing Time: 59.09 seconds

Status: Success

Environment: IntellVM

[Recreate Task](#)

[Recreate Task with Detailed Capture](#)

Sample Details

Sample ID: 2488

Filename: Order_Pdf_...exe

MD5: ab23d60a7806c6aac1445cc545d37bdd

SHA256: 39833c40bfa9ac0bab5f058c208dfe3663062b39cd609aa655e7af238c399as

Filetype: PE32 executable for MS Windows (GUI) Intel 80386 32-bit

[Download Sample](#)

Filter Detections:

- Creates process in suspicious location
- Adds Autostart Object

Virus Total Info

At least 4 security vendors detect this file in some form

Please [click here](#) to see the result from Virus Total

PCAP File

[4635-ab23d60a7806c6aac1445cc545d37bdd.pcap](#)

Event Distribution Chart

Activity Report [View Full Event List](#) | [View Event Time line](#)

Event

- Creates event DINPUTWINMM
- Creates event Globaluserenv: User Profile setup eventE1

Mutex

- Creates mutex SHIMLIB_LOG_MUTEX
- Creates mutex 337009189

Process

- Creates process C:\WINDOWS\Temp\ab23d60a7806c6aac1445cc545d37bdd.exe
- Creates process C:\WINDOWS\system32\svchost.exe

Semaphore

- Creates semaphore shell,{A48F1A32-A340-11D1-BC6B-00A0C90312E1}17bdd.exe
- Creates semaphore shell,{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

Filesystem

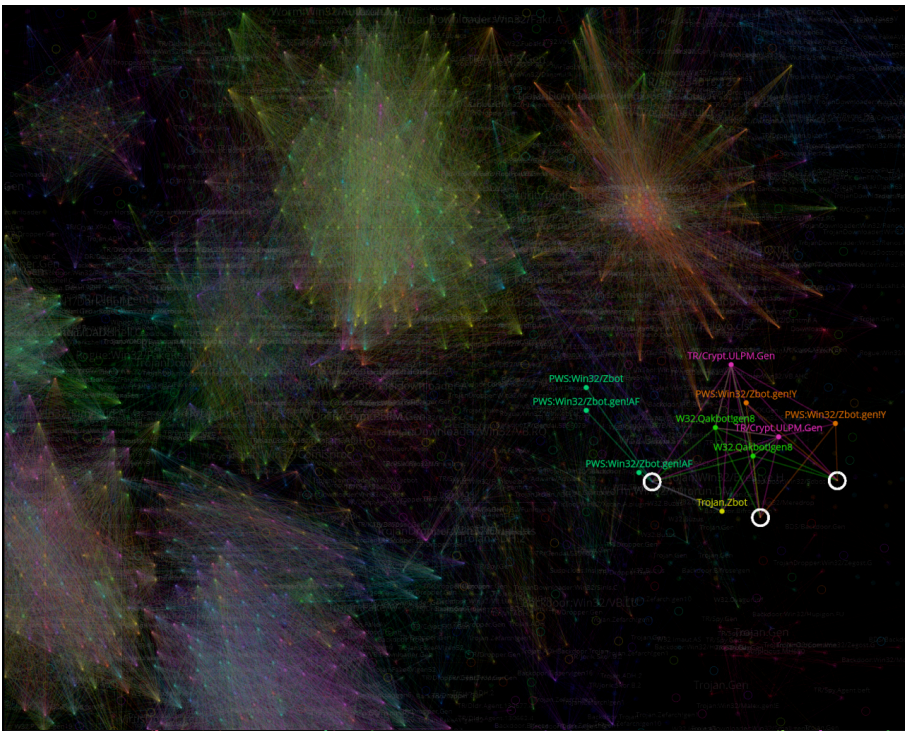
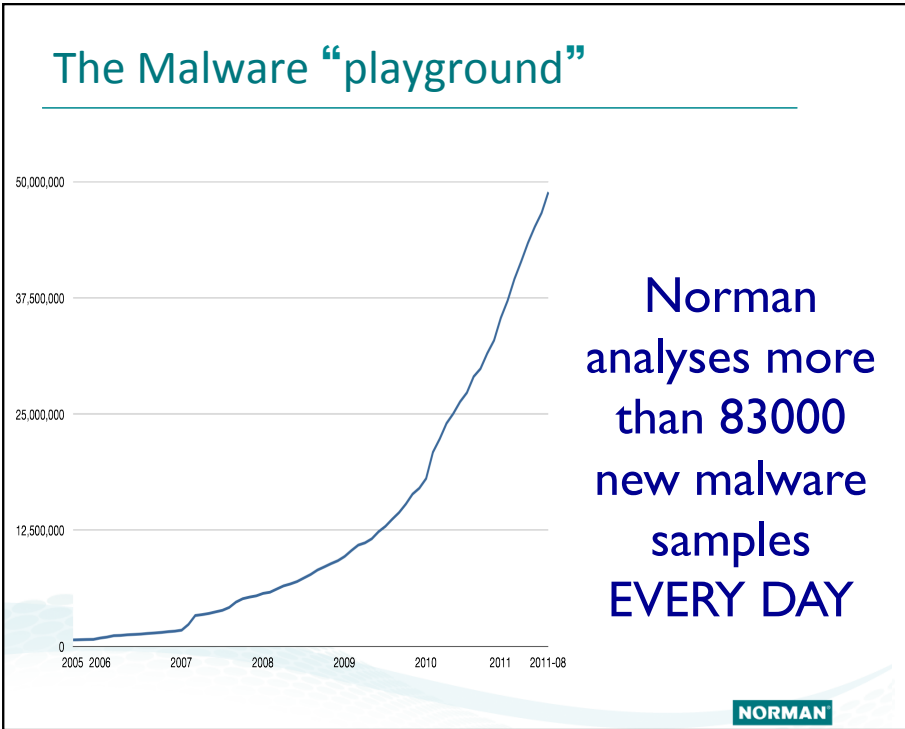
- Creates file c:\Documents and Settings\All Users\Local Settings\Temp\0e677f1f0000f198.exe (FILE_OVERWRITE_IF)
- Opens file c:\Documents and Settings\All Users\Local Settings\Temp\0e677f1f0000f198.exe (FILE_OPEN)
- Writes to file c:\Documents and Settings\All Users\Local Settings\Temp\0e677f1f0000f198.exe

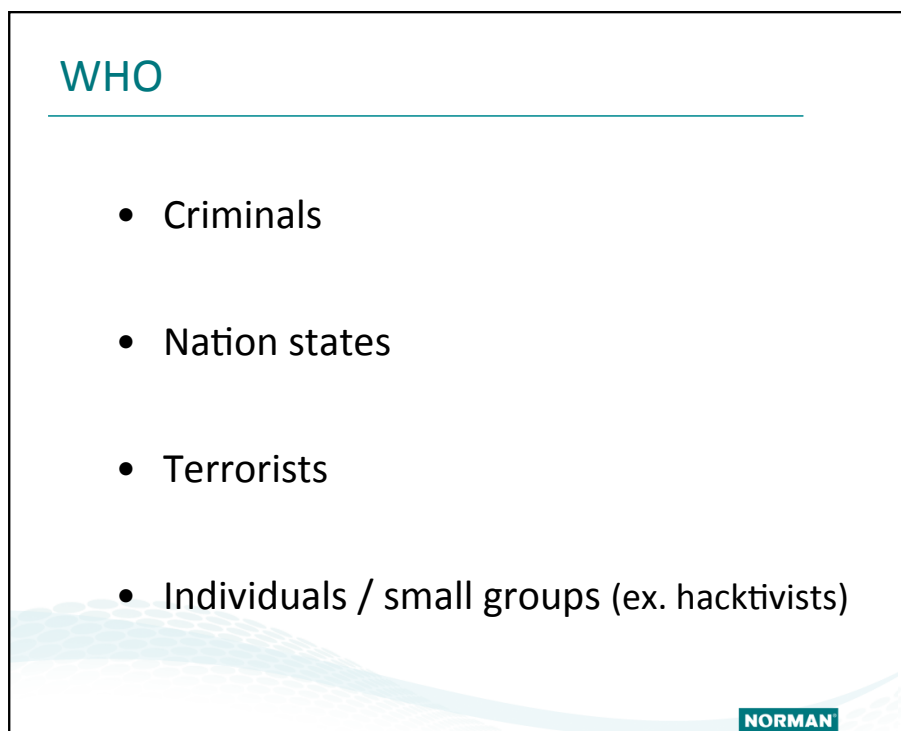
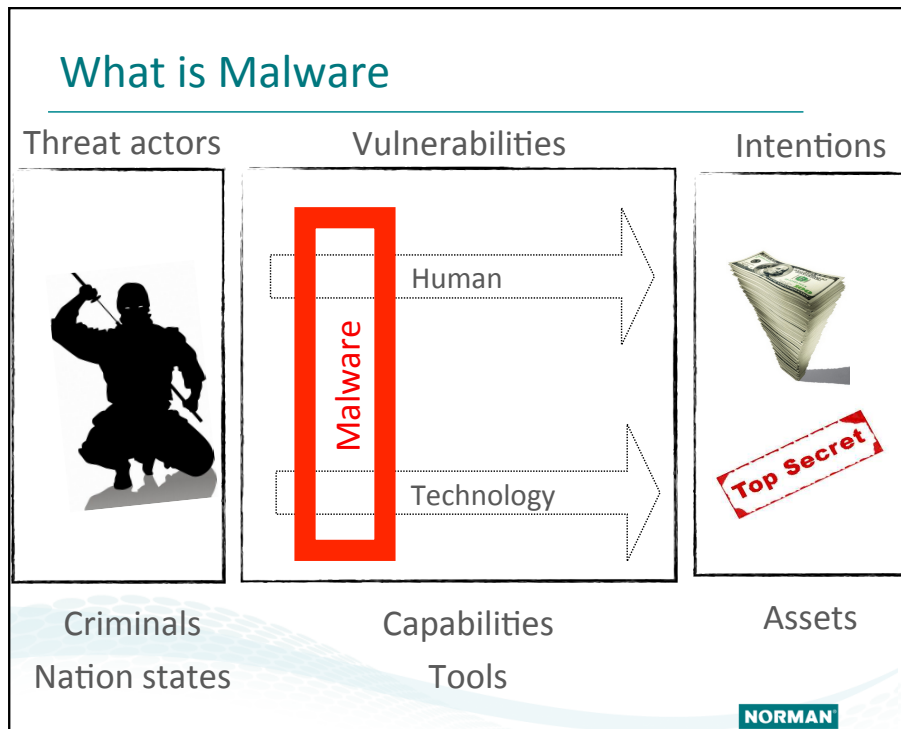
Network

- Tries to resolve heppishopdrn.ru
- Exchanges data with 8.8.4.4 on port 53
- Exchanges data with 8.8.8.8 on port 53
- Connects to 8.8.4.4 on port 53
- Connects to 8.8.8.8 on port 53

Registry

- Adds/Sets value HKLM\Software\microsoft\windows\currentversion\policies\explorer\run [61848]
- Creates key HKLM\Software\microsoft\windows\currentversion\policies\explorer\run





WHO

WANTED
BY THE FBI

Wire Fraud; Conspiracy to Commit Computer Fraud; Computer Fraud

BJORN DANIEL SUNDIN



Photograph taken
in 2003

ETTERLYST AV FBI: Svenske Bjorn Daniel Sundin risikerer 480 års fengsel om han noensinne blir stilt for en amerikansk domstol.
Foto: FBI

Ifølge tiltalen i USA startet Sundin selskapet Innovative Marketing som solgte virusbeskyttelse til privatpersoner. Programmet de solgte beskyttet ikke mot noe som helst, og mellom 2006 og 2008 håvet Sundin og hans partner inn verdier for rundt 1,4 milliarder svenske kroner.

NORMAN

GROUP-IB

Cybercrime investigation

LEADING RUSSIAN SECURITY FIRM GROUP-IB RELEASES 2011 REPORT ON RUSSIAN CYBERCRIME

Russian Mafia Organizes Russian Cybercrime Market, Doubles in Size

Key Trends in 2011:

- **Russian Cybercrime Doubles:** The global cybercrime market was more than \$12.5 billion in 2011. The global Russian speaking component of that market was more than \$4 billion; and the Russian national cybercrime market was \$2.3 billion, essentially doubling last year's number of \$1.2 billion.
- **Mafia Professionalizes Russian Cybercrime:** Traditional crime syndicates are beginning to organize the previously disorganized Russian cybercrime market. In addition, these crime syndicates are beginning to work more closely together, sharing compromised data, botnets, and cashing schemes.
- **Online Fraud and Spam Account for More than Half of Russian Cybercrime:** In 2011, the largest type of Russian cybercrime was online fraud at \$942 million; followed by spam at \$830 million; cybercrime to cybercrime, or C2C (including services for anonymization and sale of traffic, exploits, malware, and loaders) at \$230 million; and DDoS at \$130 million.

WHY – ADVANCED ATTACKS / ESPIONAGE

Advanced Persistent Threat (APT)

Advanced = it gets through your existing defense.

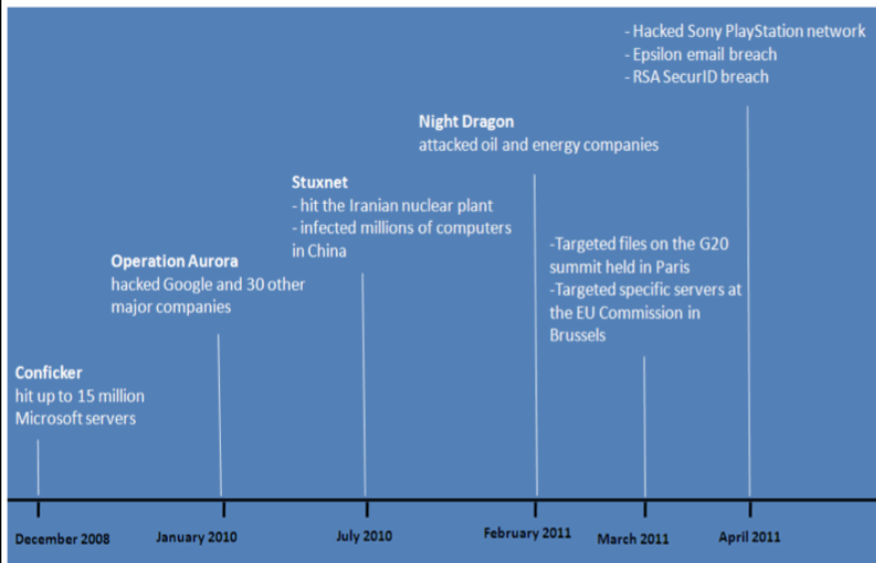
Persistent = it succeeds in hiding from your existing level of detection.

Threat = it causes you harm (threat actors with capabilities and intent)

Gartner Aug'11

NORMAN

Major APT incidents



Source: Ahnlab

WHAT CAN WE EXPECT ?

- Why do you rob banks?
 - “Because that’s where the money is.”

Willy Sutton

Expect:

- More cyber crime, profesionalized
- More advanced attacks
- Attacks targeting smartphones / tablets
- Attacks on industrial systems

NORMAN

2012 Cybercrime trends

- **Trend #1: The Trojan Wars Continue**
 - Banking trojans (Zeus, SpyEye, etc.)
 - Mobile platform trojans
- **Trend #2: Cybercriminals will Find New Ways to Monetize Non-Financial Data**
 - Currently: spam mailing lists, dates of birth (DOB), and unfiltered Trojan logs.
- **Trend #3: Fraud-as-a-service**
 - elaborate sets of compromised credit cards, account logins, trojans for sale, botnets for rent,...
- **Trend #4: Out-of-band Methods**
- **Trend #5: The Rise of Hacktivism**

RSA 2012 CYBERCRIME TRENDS REPORT **NORMAN**

What does the IT security industry do ?

Traditional protection such as AV and FW is not enough.

Defense in Depth — Layered security


NORMAN

Advice to deal with the threat picture

- **Endpoint security – a secure baseline:**
 - Reduce vulnerability with application and device control and patch management
 - Updated antivirus
- **Network Security Monitoring**
 - Network analysis / context information
 - Network appliances for malware detection, analysis and prevention
- **Detect, react, mitigate**
 - Incident response and Malware analysis tools

NORMAN

Advice to deal with the threat picture

- Endpoint security – a secure baseline:
 - Reduce vulnerability with application and device control
Norman Device Control
 - and patch management
Norman Application Control
 - Updated antivirus
Norman Patch & Remediation
Norman Endpoint Protection
- Network Security Monitoring
 - Network analysis / context information
 - Network appliances for malware detection, analysis and prevention
Norman Network Protection
- Detect, react, mitigate
 - Incident response and forensic analysis tools
Norman Malware Analysis G2 

Thank you!

Christophe Birkeland

cbi@norman.com

