NORMAN

Spionasje og mobilitet

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)
- Markets: Consumers, Business, Government, OEM, Industry
- 40.000 Business Customers
- Over 2500 Partners worldwide
- Strong partnerships with key industry leaders

NORMAN

A Global Security Player

Technology Leader in Malware Analysis & Threat Defence

- Launched Norman SandBox in 2005
- Launched SandBox Malware Analyzer in 2007
- Launched Norman Network Protection in 2008
- Awarded *"Most Innovative idea in 10 years"* in 2010 for Norman SandBox
- Launched Malware Analyzer G2 in 2011
- Launched Norman SCADA Protection in 2012

Overview

- TRENDS:
  - SOCIETY
  - TECHNOLOGY / MOBILITY
  - THREAT PICTURE
- ADVICES

NORMAN

Trends – A Digital Society

- Everything is interconnected
  - Information systems / data storage
  - More and more physical processes (access control, most industrial systems, your car, etc.)
- "Coming up" – Internet of things

NORMAN

Important trends – Consumerization

"New information technology emerges first in the consumer market and then spreads into business and government organizations."

- BYOD
- Employees and departments are becoming self-sufficient in meeting their IT needs (cloud services)
- Companies depend more and more on consumerized services (email, CRM, Intranet, backup, collaboration, …)

NORMAN

Mobile computing – Trends

- Tremendous growth of smartphones / tablets, multiple devices / platforms
- Huge improvements in apps and browsers
- Wireless networks are faster and more reliable
- Risk Challenges are Evolving – Security issues
- Mobile Computing is Revolutionizing How Work is Done – Today's generation Y lives mobile/wireless life
- Mobile Computing is Here to Stay Whether People or IT are Prepared or Not

NORMAN

HorizonWatching, January 17, 2012

Trends – The Cyber Threat Picture

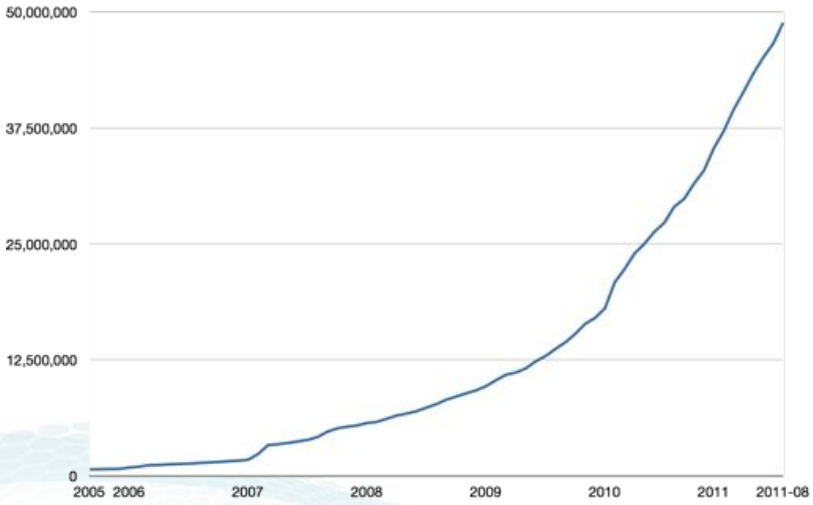
- What is malware ?
- WHO & WHY
- Advanced Persistent Threat (APT)
- Threats to industrial systems

NORMAN

What is malware?

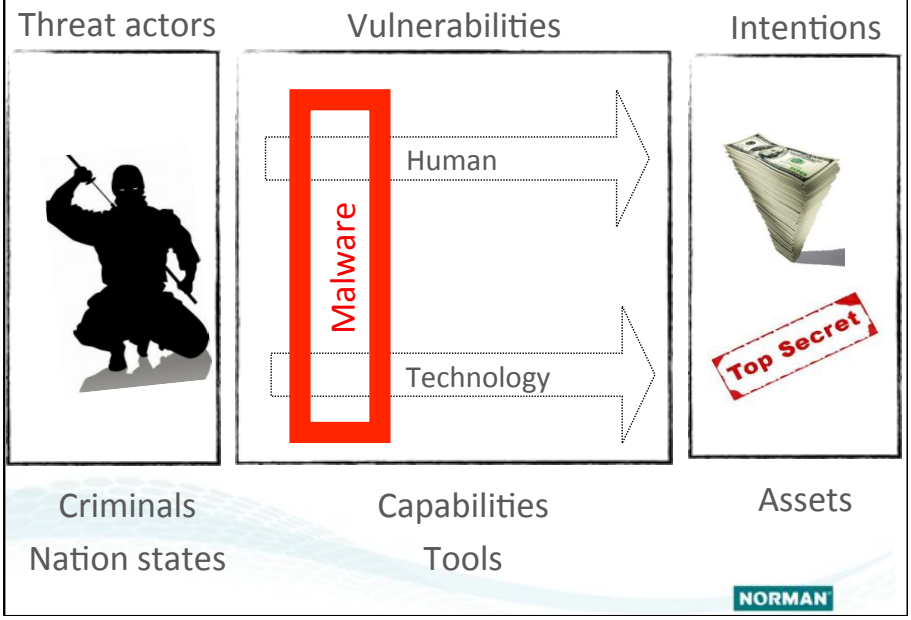
Norman Malware Analysis Generation 2

The Malware "playground"



NORMAN

What is Malware



NORMAN

WHO

- Criminals
- Nation states
- Terrorists
- Individuals / small groups (ex. hacktivists)

NORMAN

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 Bjørn 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

WHO

NORMAN

WHY

NORMAN

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 (cont.)

RSA (*RSA's SecurID two-factor authentication*):

- Lockheed Martin
- L-3 Communications
- Northrop Grumman
- Other Defense contractors
- …

"Shady RAT" *(targeted attacks on more than 70 global companies)*

NORMAN

Angrepet på nettsiden skjer etter at fredsprisen til den kinesiske menneskerettighetsaktivisten Liu Xiaobo har fått stor oppmerksomhet internasjonalt.

Nobelkomitéens nettsider hacket

Angrepet fra taiwansk ip-adresse.

PER ANDERS JOHANSEN, LARS AKERHAUG

Skriv ut Tips en venn

MAN

Attacks on Industrial Systems (SCADA)

NORMAN

Unintentional threats for ICS

Common malware not targeting ICS/SCADA

- Affects stability and availability = decreased up-time
- May damage brand / company image
- Clean-up time by itself can cause massive financial losses
- More likely to be hit by generic malware than targeted malware

"Common malware" threats

Nuclear reactor (US, Ohio Davis-Bess nuclear power station)
Reactor network slows down and the security and monitoring systems stay off-line for almost 5 hours
Cause: Malware (Slammer) infected systems through a consulting company's private T1 line that circumvented the network firewall
Cost: $600.000

Australian Railway
300.000 commuters in greater Sydney area without transportation an entire day
Cause: Malware compromised the signal and control systems
Cost: Unknown, but estimated in the millions

Daimler Chrysler (US)
13 production plants shut down for over 1 hour. Up to 50.000 workers without anything to do..
Cause: Malware compromised un-patched Windows 2000 systems
Cost: $14 mill. (estimated)

Intentional threats for ICS

Stuxnet – first wildly known malware targeting ICS

Made of many components

- Spreading vectors / exploits
- Peer-to-peer communication (in LAN)
- Windows rootkit (signed)
- PLC rootkit (SCADA)
- Command and control interface

Initial spreading vector was USB sticks exploiting the Microsoft Windows LNK vulnerability

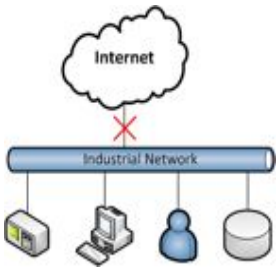
Duqu – son of Stuxnet?

Information stealing trojan
Similar code to Stuxnet

NORMAN

Network Security in Industrial Environment

Easy way (naive):



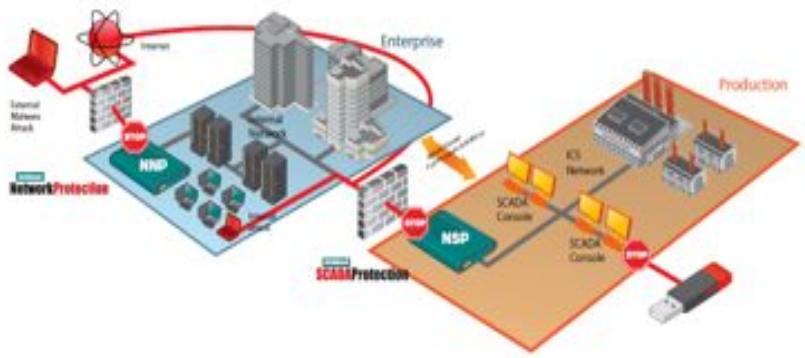
However:

- Internal threats still exists.
  - Computer Security Institute estimates that 60-80% of network misuse comes from inside the enterprise.
- Network services are more and more depending on Internet
  - Patches
  - Logging from offshore to onshore facilities
  - Time synchronization
  - Weather data
  - Remote support

NORMAN

Norman SCADA Protection

Prevent cyber attacks from inside and outside the control system network



NORMAN

Advice to deal with the threat picture

- Secure Design – Defense in Depth – Layered security
- 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)
  - Malware analysis tools

NORMAN

Advice to deal with the threat picture

- Secure Design – Defense in Depth – Layered security
- Endpoint security – a secure baseline:
  - Reduce vulnerability with application and device control and patch management
  - Updated antivirus

Norman Device Control
Norman Application Control
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)
  - Malware analysis tools

Norman Malware Analysis G2 NORMAN

Thank you!

Christophe Birkeland

cbi@norman.com

NORMAN