

GOVCERT.NL en de aanpak van ICT-dreigingen

Een kijkje in de keuken

ISACA Roundtable 2 Februari 2009

Agenda

- > GOVCERT.NL
- > Samenwerking met de vitale sectoren
- > De ontwikkelingen op het gebied van cybercrime

GOVCERT.NL

GOV Government

C Computer
E Emergency
R Response
T Team

.NL Nederland



GOVCERT.NL

CERT/CSIRT

Reactive Services



- + Alerts and Warnings
- + Incident Handling
 - Incident analysis
 - Incident response on site
 - Incident response support
 - Incident response coordination
- + Vulnerability Handling
 - Vulnerability analysis
 - Vulnerability response
 - Vulnerability response coordination
- + Artifact Handling
 - Artifact analysis
 - Artifact response
 - Artifact response coordination

Proactive Services



- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services



- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

Zie: www.cert.org

Preventie

Monitoring

Deelnemers &
publiek



Informatie-
knooppunten



GOVCERT.NL

(inter)nationale
partners

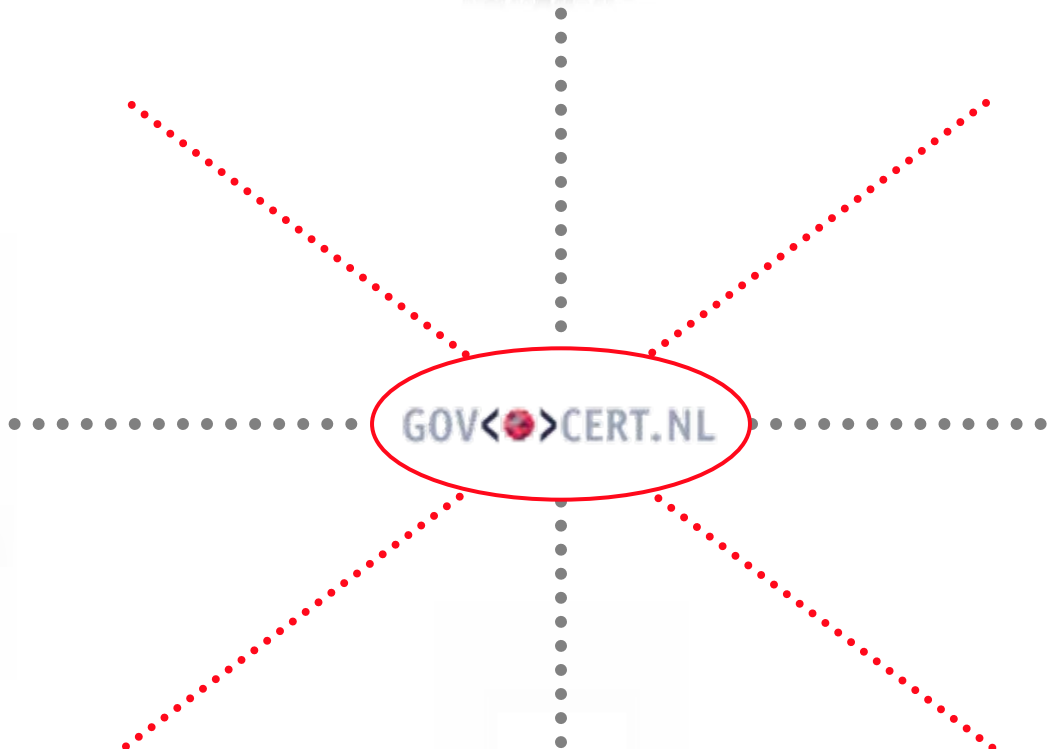


Kennisuitwisseling

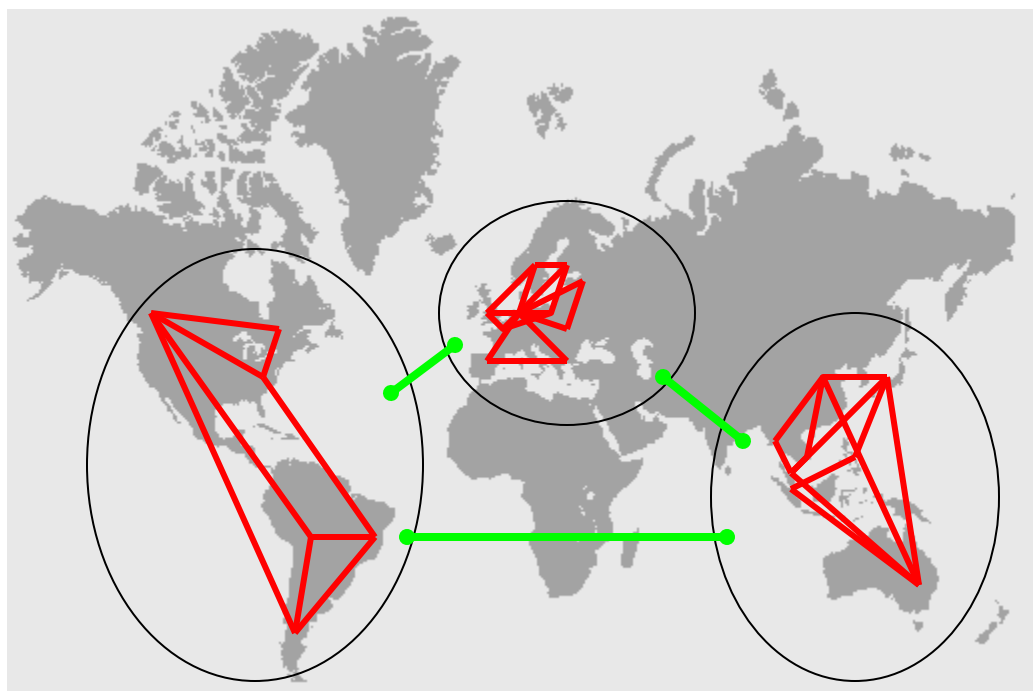
Respons



ISP's



(Inter)nationale partners



-  AIVD
O-IRT-O
KLPD
NICC
-  EGC
TF-CSIRT
ENISA
-  FIRST
APCERT
OAS

Preventie

Deelnemers & publiek



Monitoring

Sensornetwerk
Early warnings
Karakteristieken van aanvallen
Statistieken

Informatie-
knooppunten



(inter)nationale
partners



GOVCERT.NL

Kennisuitwisseling



ISP's

Respons

Preventie: advisory

```
#####
## GOVCERT.NL ~ BEVEILIGINGSADVIES ##
#####

Titel           : Nieuwe kwetsbaarheid in Plug and Play
Advisory ID     : GOVCERT.NL-2005-298
Versie          : 1.0
Risico          : medium
CVE ID          : CAN-2005-2120
                 (http://cve.mitre.org/cve/)
Schade          : high
                 Lokale root-rechten
                 Uitvoeren van willekeurige code op afstand
Auteur          : ██████████
Uitgiftedatum  : 20051011
Toepassing      : Microsoft Windows 2000 (alle versies)
                 Microsoft Windows XP (alle versies)
Versie(s)       :
Platform(s)     : Microsoft Windows
Beschikbaarheid: https://kennisbank.govcert.nl/

Samenvatting
  In Plug and Play (PnP) van Microsoft Windows 2000 en XP is een
  nieuwe kwetsbaarheid gevonden. Microsoft heeft updates beschikbaar
  gesteld waarmee deze kwetsbaarheid wordt opgelost.
```


Preventie



Gratis services

- E-mail Alert
- SMS Alert
- Nieuwsbrief



ABCDEFGHIJKLMNOPQRSTUVWXYZ

Access Point

Een Access Point (AP) is een apparaat dat radiosignalen met netwerkverkeer opvangt en deze verder verstuurt over een vaste lijn. Het geeft iemand met een draadloze netwerkkaart dus toegang tot een vast netwerk, zoals het internet. Access Points worden vaak in één apparaat gecombineerd met routers of switches: dit zijn de wireless routers die tegenwoordig erg populair zijn.

Active Directory

De Active Directory is een database waarmee beheer van gebruikers en toegang tot diensten en bestanden binnen Microsoft Windows netwerken kan worden geregeld.

ActiveX

ActiveX is een verzamelnaam voor een aantal onderdelen, waaronder het bekijken van PDF-bestanden in uw browser, zonder ze apart te hoeven downloaden. Onder Active X vallen bijvoorbeeld ActiveX-controls, maar ook Active Scripting en de Java Virtual Machine, de Java "vertaler" waarvan Internet Explorer gebruik maakt.

Are you master of your own identity?

Vult u overal op internet zomaar uw gegevens in? Of werkt u juist met verzonnen namen en niet bestaande adressen? Had de man in de film 'Are you master of your own identity' dat maar gedaan..!

Digitale dreigingen thuis

Waarschuwingsdienst.nl heeft een film geproduceerd die als doel heeft mensen bewust te maken van de risico's van het internet. Centraal thema van deze film is dat je je vooral bewust moet zijn van je eigen gedrag.

Botnet film

Waarschuwingsdienst.nl toont de gevaren van virussen, wormen en botnets – netwerken van geïnfecteerde PC's gebruikt voor criminele doeleinden – in een nieuwe animatiefilm.

Vachtwoordenfilms

Vachtwoorden, je hebt er inmiddels zoveel in gebruik, je wordt er gek van! Toch is het raadzaam bewust en waakzaam om te springen met het gebruik en toepassen van je wachtwoorden...

Maar is Chris?

Deze korte film laat zien waar 'normaal' gedrag op internet in het echt toe zou kunnen leiden...

dienstbeschrijving> <disclaimer> <privacy>

erheid.
atie over
zen over
ze dienst
gsekken in

TOP 10 TIPS

zoeken...

GO

Gratis alerts!



Preventie

Waarschuwingen ("advisories")
Adviezen
Waarschuwingsdienst.nl

Deelnemers &
publiek



Monitoring

Sensornetwerk
Early warnings
Karakteristieken van aanvallen
Statistieken

Informatie-
knooppunten



GOVCERT.NL

(inter)nationale
partners



Kennisuitwisseling



ISP's

Respons

GOVCERT.NL: kennisuitwisseling



Preventie

Waarschuwingen ("advisories")
Adviezen
Waarschuwingsdienst.nl

Deelnemers &
publiek



Monitoring

Sensornetwerk
Early warnings
Karakteristieken van aanvallen
Statistieken

Informatie-
knooppunten



GOVCERT.NL

(inter)nationale
partners



Kennisuitwisseling

Kennisbijeenkomsten / symposium
White papers / Factsheets
Kennisbank, netwerken
Samenwerking binnen overheid



ISP's

Respons

Ondersteuning bij incidenten
7x24 uur waakdienst
Bestrijden gevolgen cybercrime

Agenda

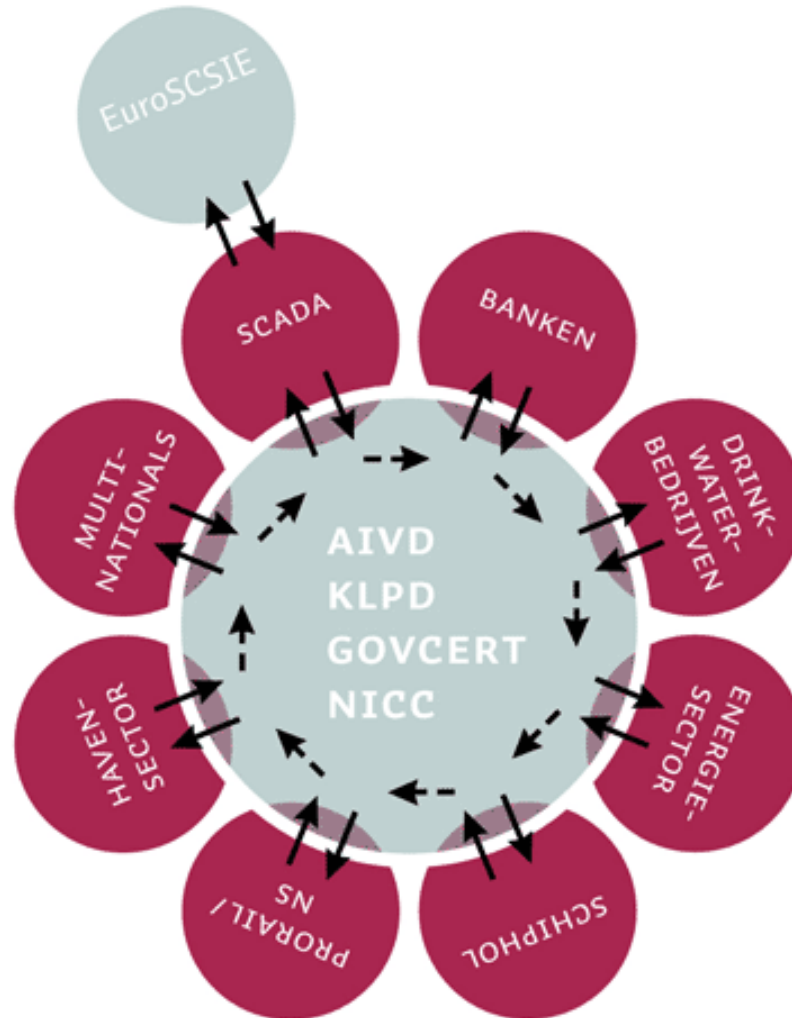
- > GOVCERT.NL
- > Samenwerking met de vitale sectoren
- > De ontwikkelingen op het gebied van cybercrime



Vitale sectoren



Informatie delen met de vitale sectoren



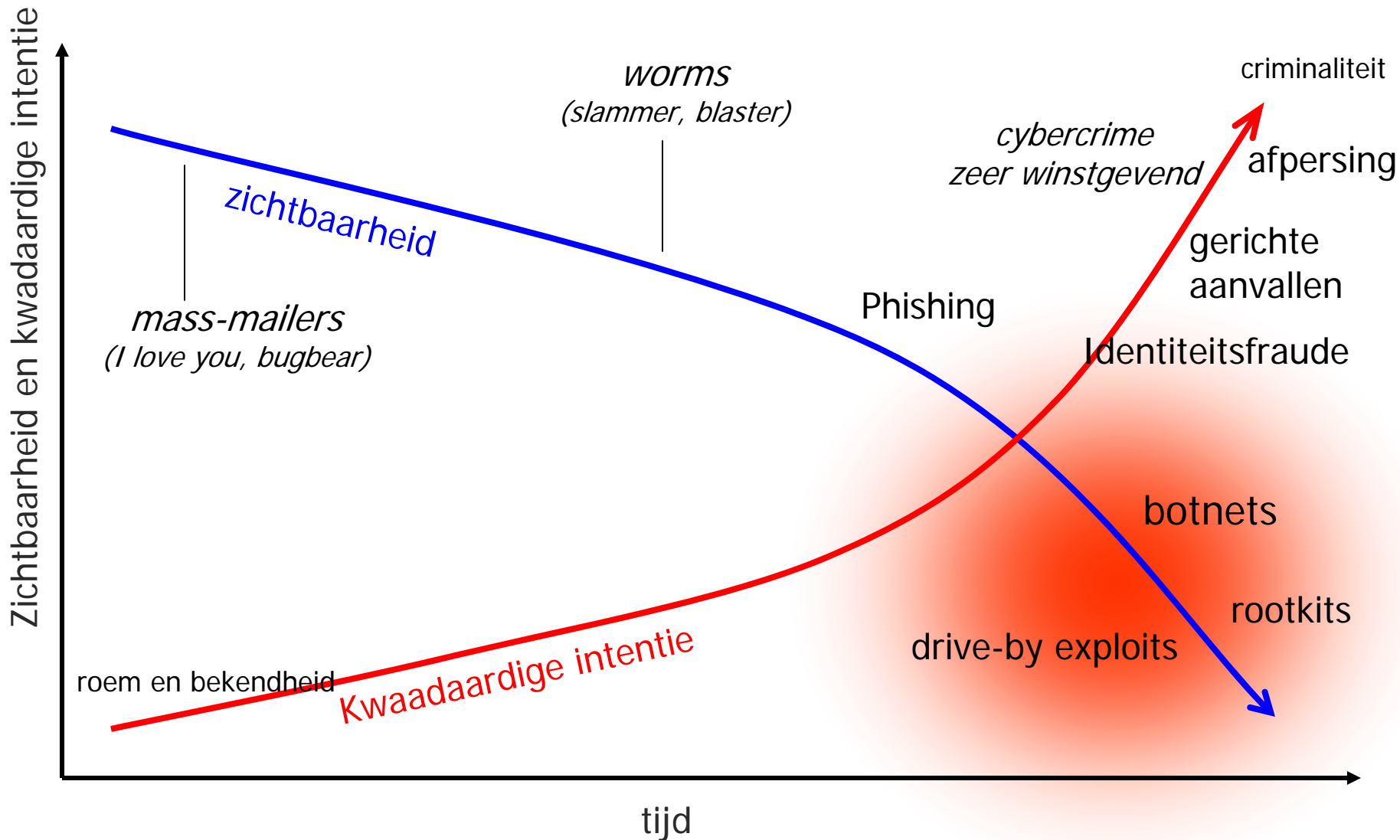
Werkt het?

- > De ene ISAC is wat 'verder' dan de ander
 - FI-ISAC heeft veel activiteiten
 - Rail-ISAC is (nog) in opstartfase
- > Alle partijen ervaren de informatiedeling als zeer waardevol
- > Enkele ISAC's nemen deel in onderzoeksprojecten en het uitbrengen van publicaties
- > Initiatieven in een ISAC zijn vaak ook waardevol voor andere ISAC's
- > Tijdsinvestering is nodig om een ISAC succesvol te maken

Agenda

- > GOVCERT.NL
- > Samenwerking met de vitale sectoren
- > De ontwikkelingen op het gebied van cybercrime

Van verleden naar heden



Ontwikkelingen

Phising op maat



The image shows a screenshot of a phishing page designed to look like the Postbank.nl login page. The page features the Postbank logo and the title 'Inloggen Mijn Postbank.nl'. It includes several sections of text and a login form. The form has four input fields: 'Gebruikersnaam', 'Wachtwoord', 'Postbank Card', and 'PIN code'. Below the form is a checkbox for 'Gebruikersnaam bewaren op deze computer'. At the bottom of the form are 'Inloggen' and 'Annuleren' buttons. Below the form, there are three more sections: 'Nieuw Gebruikersnaam en/of Wachtwoord aanvragen?', 'Heeft u nog geen Mijn Postbank.nl?', and 'Meer informatie over:'. The page is styled with a light blue background and dark blue text.

Postbank

Inloggen Mijn Postbank.nl

Veilig Bankieren
[Meer over veilig bankieren met Mijn Postbank.nl.](#)

Hoe kan ik blokkering van mijn gebruikersnaam en wachtwoord voorkomen?
[Meer informatie over het voorkomen van blokkering](#)

Dit weekend vindt er onderhoud plaats aan Mijn Postbank.nl
Klik hier voor [meer informatie over het onderhoud.](#)

Gebruikersnaam

Wachtwoord

Postbank Card

PIN code

Gebruikersnaam bewaren op deze computer [?](#)

Inloggen **Annuleren**

Nieuw Gebruikersnaam en/of Wachtwoord aanvragen?
[Nieuw Wachtwoord en/of Gebruikersnaam aanvragen](#)

Heeft u nog geen Mijn Postbank.nl?
[Mijn Postbank.nl aanvragen](#)
[Zakelijk Mijn Postbank.nl aanvragen](#)

Meer informatie over:
[Postbank NV](#)
[Mijn Postbank.nl](#)



Polymorfe malware



Nep anti-virus

The screenshot displays a Windows XP desktop environment. The desktop background is blue. On the left side, there is a vertical taskbar with icons for 'My Documents', 'My Computer', 'My Network Places', 'Mozilla Firefox', 'Internet Explorer', 'Windows', and 'Antivirus 2008'. The main window is a web browser displaying the 'Antivirus XP 2008' product page. The page has a blue header with the product name 'Antivirus XP 2008' in white and yellow text. Below the header, there are two yellow boxes containing pricing information. The first box shows 'EUR 49.95' with a 'Pay by credit card' button. Below this, it lists 'Antivirus XP 2008 Standard edition + 1 year free updates' and 'Scanner + Spyware Remover + Real-Time Protection + bonus features'. The second box shows 'EUR 99.95' with a 'Pay by credit card' button, listing 'Antivirus XP 2008 Standard edition + 3 years free updates' and the same features. Below these boxes, there is a section titled 'Instant Access, Discreet Billing, Secure Procedure by conveniently using our Online Credit Card Option.' followed by '5 good reasons to buy now:' and a bulleted list: '24/7 qualified customer support service', 'Progressive technology in action', 'Customer satisfaction and money back guarantee', 'Free Antivirus XP 2008 Membership', and 'User friendly interface'. At the bottom of the browser window, there is a 'SAFETY SECURITY' banner. The Windows taskbar at the bottom shows the Start button, Google - Mozilla Firefox, Downloads, and Antivirus XP 2008. The system tray on the right shows the Internet icon, a volume icon, and the time 10:04.

File Edit View Favorites Tools Help

My Documents Antivirus XP 2008

Antivirus XP 2008

Buy

EUR 49.95 [Pay by credit card](#)

Antivirus XP 2008 Standard edition + 1 year free updates
Scanner + Spyware Remover + Real-Time Protection + bonus features
PRICE:EUR 49.95 (This is a One Time Only Charge, your credit card will never be rebilled and you will receive UPGRADES FOR FREE!)

EUR 99.95 [Pay by credit card](#)

Antivirus XP 2008 Standard edition + 3 years free updates
Scanner + Spyware Remover + Real-Time Protection + bonus features
PRICE:EUR 99.95 (This is a One Time Only Charge, your credit card will never be rebilled and you will receive UPGRADES FOR FREE!)

Instant Access, Discreet Billing, Secure Procedure by conveniently using our Online Credit Card Option.

5 good reasons to buy now:

- 24/7 qualified customer support service
- Progressive technology in action
- Customer satisfaction and money back guarantee
- Free Antivirus XP 2008 Membership
- User friendly interface

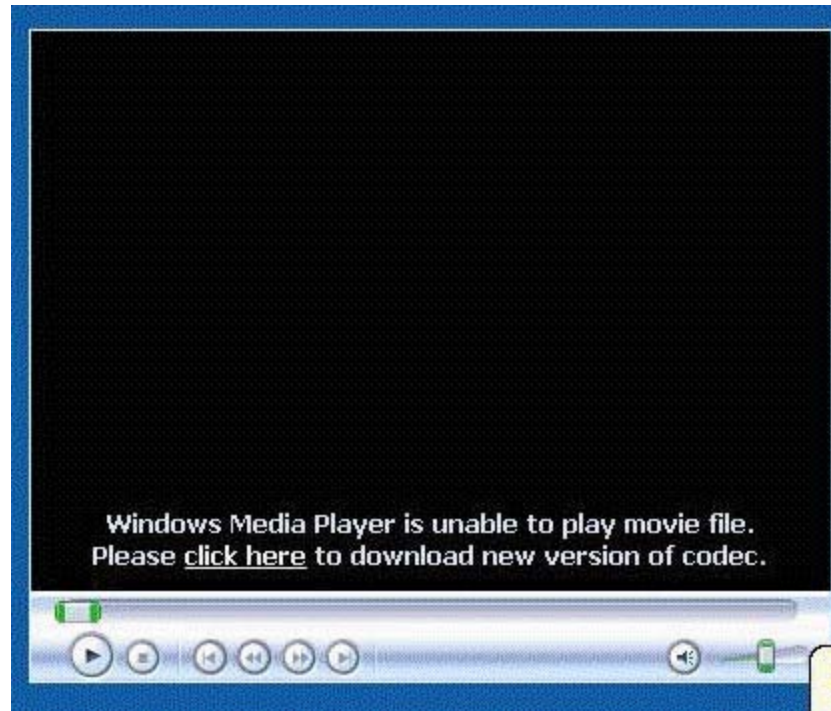
Done

Internet 100%

Start Google - Mozilla Firefox Downloads Antivirus XP 2008 Antivirus XP 2008 - W... EN 10:04

Start Google - Mozilla Firefox Downloads Antivirus XP 2008 EN 10:03

Nep-codecs





Infecteren vertrouwde sites

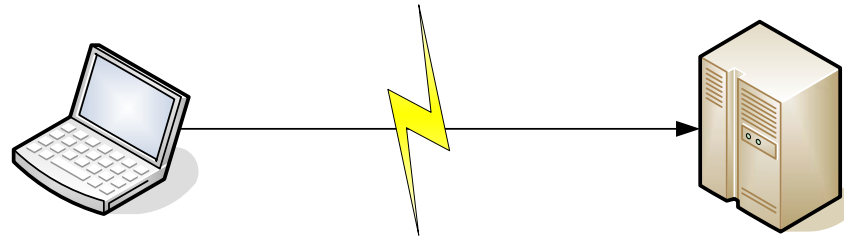


bloomingdale's





Man in the browser



Fast-flux netwerken

Zeer snelle wisseling van de internet-adressen van kwaadaardige systemen





Nieuwste ontwikkelingen

- > Toename van applicatie gerichte malware
 - PDF, Flash, Quicktime, ...
- > Detectie van Virtualisatie
- > Imitatie-hardware met malware
- > Malware gericht op printers & copiers



Hoe hiertegen te wapenen?

- > Houd software up to date en patch, patch patch
- > Zorg voor anti-virus/malware software
- > Beveilig de eindpunten
- > Train de gebruikers: **weersta de verleiding, weet waarop je klikt!**
- > Zorg voor goede informatie : **Inzicht vergroot alertheid**

Vooruitblik 2009







РЕВКАС



Vragen?

Links

www.govcert.nl

www.waarschuwingsdienst.nl

www.samentegencybercrime.nl

Informatieknooppunten: nicc@ictu.nl

info@govcert.nl