GOVCERT.NL en de aanpak van ICT-dreigingen

Een kijkje in de keuken

ISACA Roundtable 2 Februari 2009

GOVCERT.NL

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

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

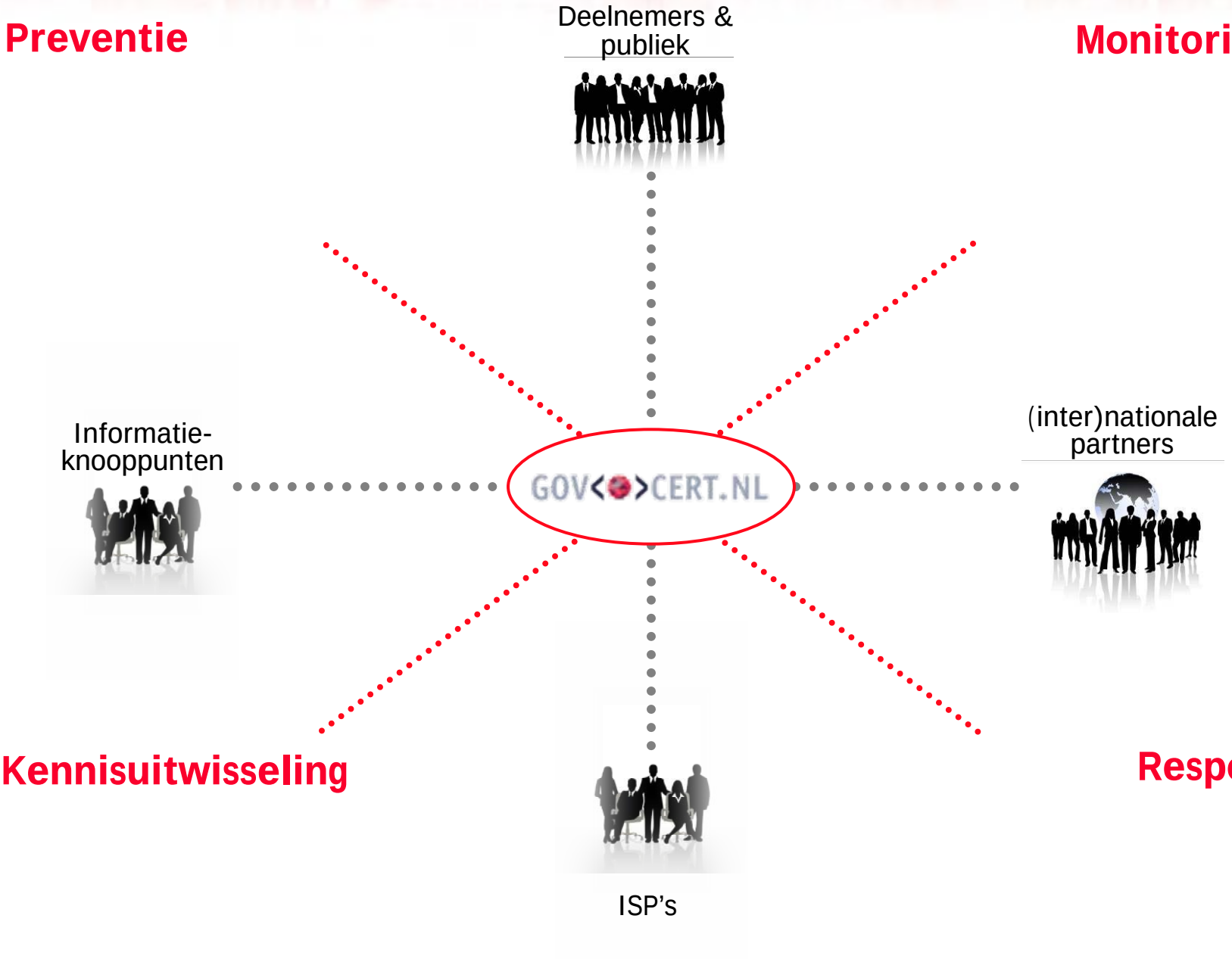
Proactive Services

- 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

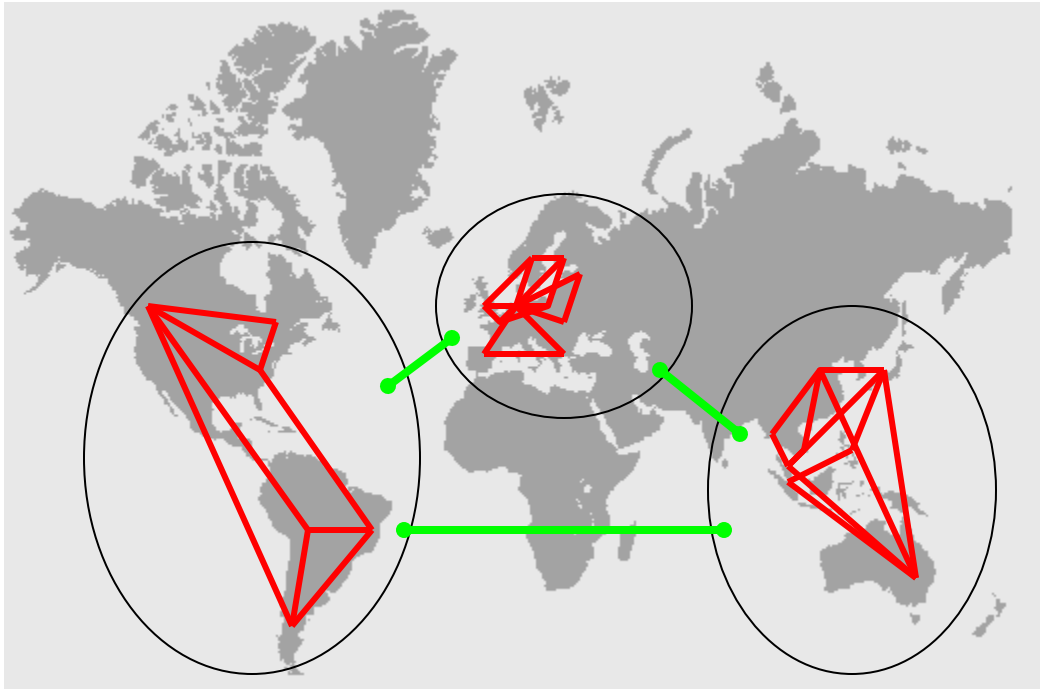
Security Quality Management Services

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

Zie: www.cert.org



(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

GOV<>CERT.NL

(inter)nationale partners

Kennisuitwisseling

ISP's

Respons

Preventie: advisory

```
   ########################################################################
  ##  G O V C E R T . N L ~ B E V E I L I G I N G S A D V I E S  ##
 ########################################################################

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          : [redacted]
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

Preventie

Waarschuwingen (“advisories”)
Adviezen
Waarschuwingsdienst.nl

Deelnemers & publiek

Monitoring

Sensornetwerk
Early warnings
Karakteristieken van aanvallen
Statistieken

Informatie-knooppunten

GOV<>CERT.NL

(inter)nationale partners

Kennisuitwisseling

Respons

ISP’s

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

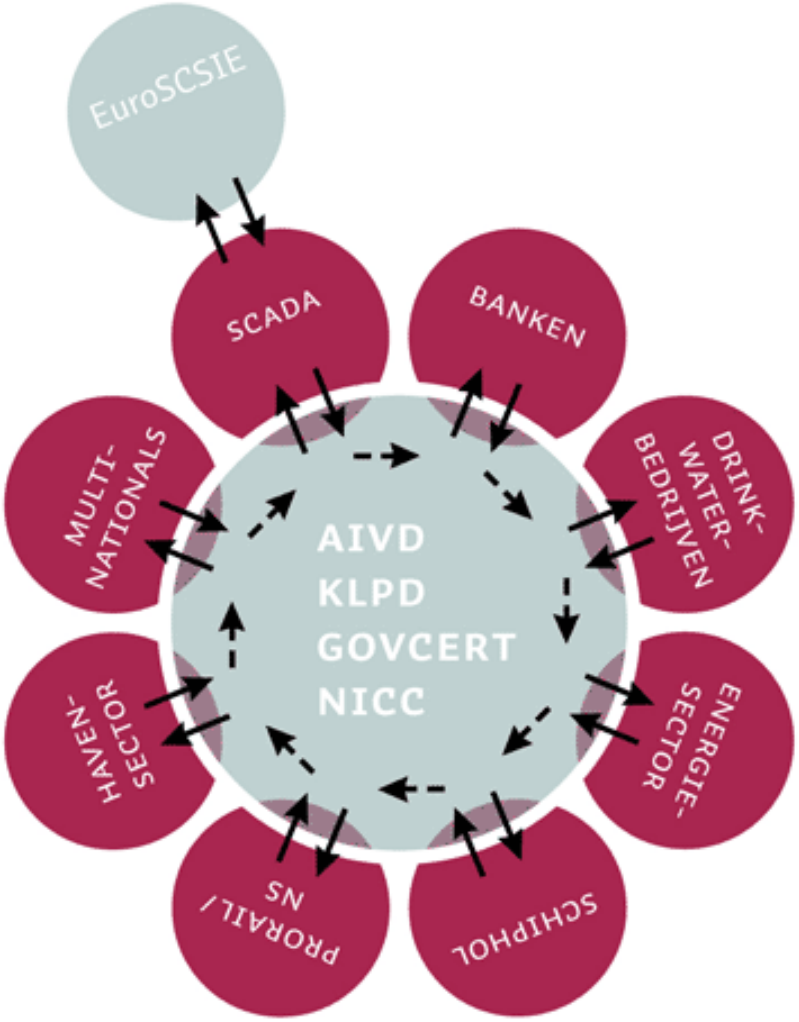
Ondersteuning bij incidenten
7x24 uur waakdienst
Bestrijden gevolgen cybercrime

Agenda

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

Vitale sectoren

Informatie delen met de vitale sectoren



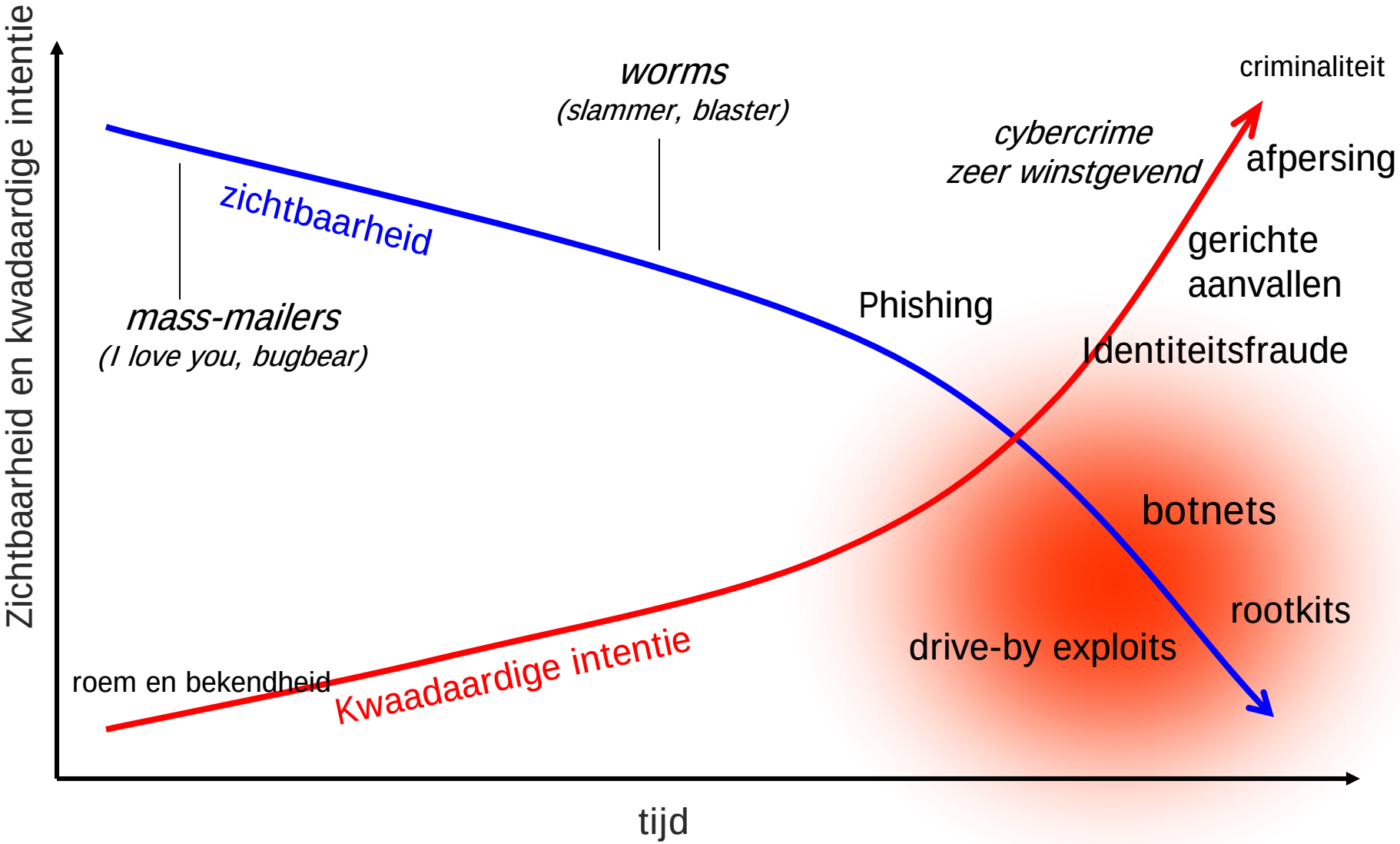
Werkt het?

- 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

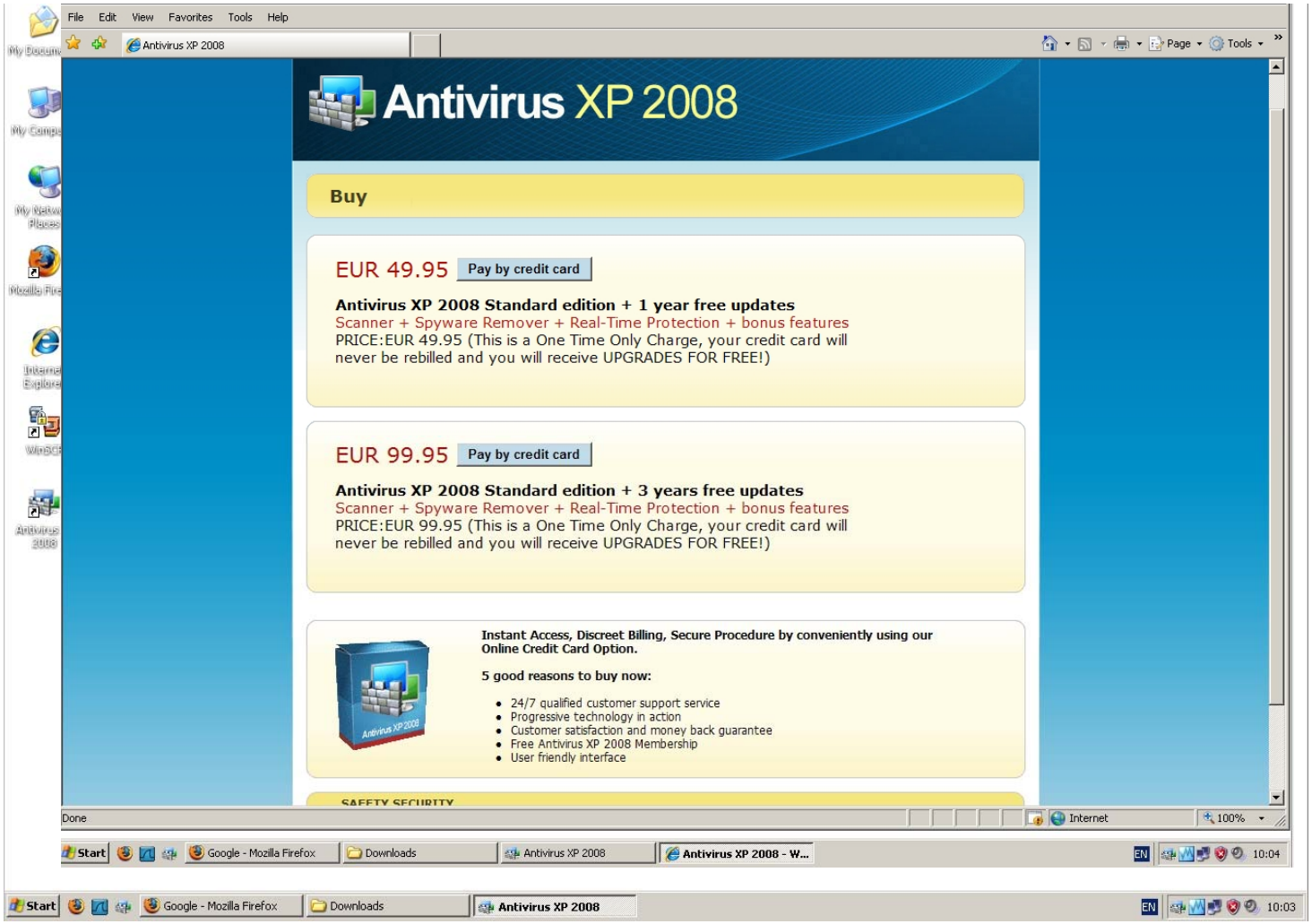


Ontwikkelingen

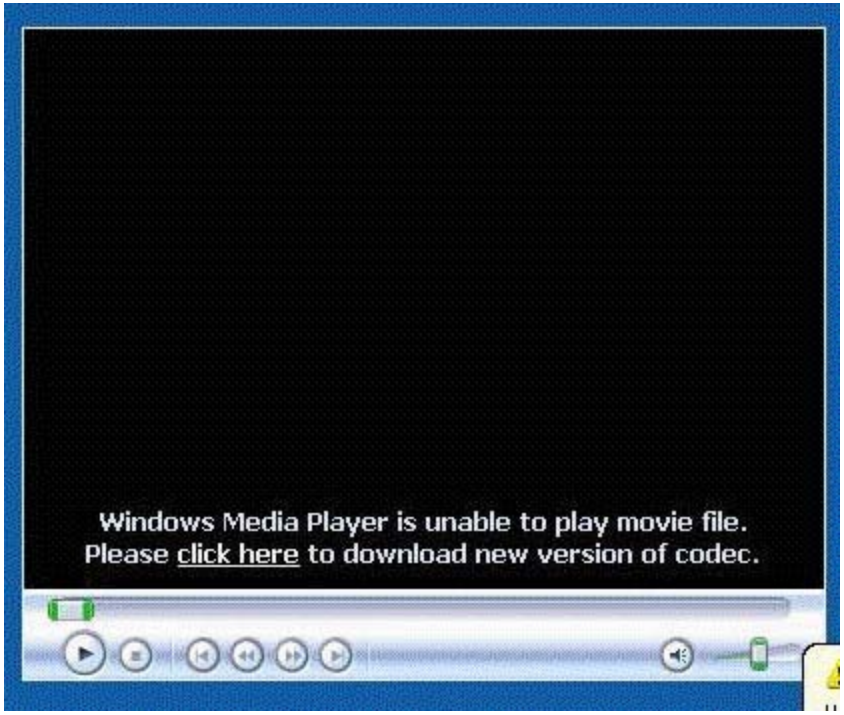
Phising op maat

Polymorfe malware

Nep anti-virus

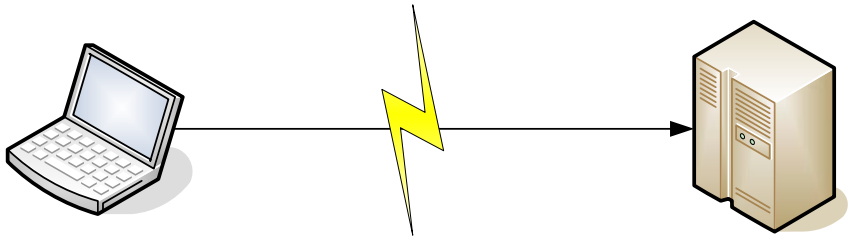


Nep-codecs



Infecteren vertrouwde sites

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

Vragen?

Links

www.govcert.nl

www.waarschuwingsdienst.nl

www.samentegencybercrime.nl

Informatieknooppunten: nicc@ictu.nl

info@govcert.nl