



# **Brainstorming & Saaldiskussion Upcoming Security Nightmares**

**oder: worüber wir nächstes Jahr lachen  
werden...**

**Berlin, den 30.12.2004**

*Moderation  
ron @ ccc.de  
frank @ ccc.de*

---



## ***Agenda***

---

**Security Nightmares, die wir haben wollen... (weil sie vielleicht was ändern)**

**Security Nightmares, die wir nicht haben wollen...**

**... to be forewarned is to be forearmed**



## Die Ironie des heise.de Banner-Servers...

heise online · c't · iX · Technology Review · Telepolis · mobil · **Security** · c't-TV · Jobs · IT-Markt · Kiosk

**TROJANER  
MÜSSEN DRAUSSEN BLEIBEN**



Hier finden Sie die Tools und Unterstützung  
für ein gut geschütztes Netzwerk ▶

Microsoft



### News

Meldung vom 28.12.2005 11:09

[<< Vorige] [Nächste >>]

#### WMF-Bilder infizieren Windows-PCs

Windows-Anwendern steht neues Ungemach ins Haus: Für eine bislang unbekannte Lücke in Windows ist ein Exploit aufgetaucht, der über ein manipuliertes Bild im WMF-Format den Rechner mit Spyware und Trojanern infiziert. Eine erste Seite ist auch bereits aktiv dabei, Besuchern Schädlinge auf die Platte zu schieben. Der Exploit lädt beim Aufruf einer präparierten Webseite mit dem Internet Explorer das Bild nach und zeigt es, je nach Konfiguration, unter Umständen automatisch in der Windows Bild- und Faxanzeige an. Dabei gelingt es dem Exploit, Schadcode ins System zu schleusen und mit den Rechten des Anwenders auszuführen. Anschließend lädt der Schadcode mehrere DLLs nach und verbiegt die Startseite des Internet Explorers. Zudem öffnet er Pop-ups mit Angeboten für Software, die den eben installierten Trojanern wieder entfernen soll.

Sponsored by



Suche

 

News

7-Tage-Alerts

7-Tage-News

News-Archive



## **Zum Aufwärmen... geplante Merchandise für die WM 2006**

---





## **Die 2004 vorhergesagten Highlights aus diesem Jahr**

---

**Superworms, Bluetooth, Instant Messaging**

**Überwachungskameras / WLAN u.a.  
Funkschnittstellen**

**Vulnerabilities in Tools rücken in den Fokus**

- Symantec, F-Secure, Trend-Micro, McAfee, Sophos, ... (Buffer Overflows im Virens scanner)
- Adobe Reader (cross platform!), Winamp, Etherreal, RealPlayer, Backup-SW, ...

**Erster Mobiltelefon / MMS Wurm (nagut, nur PoC)**

**MacOS X (erster Trojaner, nur PoC)**

**MSFT Fokus auf Security bringt Ergebnisse?!**

- der Nachteil: Clippy hilft bald beim Beseitigen von Buffer Overflows in MS Visual C++
- Proteste des Süd-Koreanischen Dienstes weil MSFT Windows 98 nicht mehr patched

**VoIP**

**OpenSource Produkte (Firefox usw.)**

**zlib everywhere**

**Kundendaten verloren haben dieses Jahr:**

**Marriott (2k), ABN Amro (2m), Time-Warner (600k), Guidance (3.8k), ChoicePoint (35k), Bank of America (1.2m), RVI (1.4m), LexisNexis (310k)...**



*... und was (noch) nicht passiert ist*

---

**Mautsysteme**

**SSH wirds nochmal dick erwischen**

**Biometrie-Großprojekte**

**ZigBee (Hausautomation, 350m Reichweite, ...)**

**mobile Bot-Netze / Würmer die Premium SMS verschicken**

**die Vernetzung von Autos / z.B. CAN Bus / RDS → CAN → Autoelektronik**

- “Handy-Wurm Cabir soll keine Gefahr für Lexus-Fahrzeuge darstellen“ (heise)

**...aber aufgeschoben ist nicht aufgehoben!**



## ***Was wir letztes Jahr (für dieses Jahr) vergessen hatten, bzw. was sonst noch war...***

---

### **SPAM / Phishing wurde tatsächlich noch schlimmer...**

- “So meldet die Paderborner Polizei einen Fall, in dem sich ein 20-jähriger Paderborner Anfang Dezember selbst anzeigte, da er sich ertappt gefühlt hatte.“ (heise)

### **Firmen greifen zu Rootkits**

- Sony erhöht die Zombie-Population um 3-500.000 PCs bei 2.1m verkauften CDs

### **php ist immer noch nicht “sicher”**

### **SHA-1 “geknackt” ( $2^{80} \rightarrow 2^{69}$ )**

### **Default Passwörter sind immer noch nicht ausgestorben**

### **Daten-Geiselnahme und Erpressung durch Virus (PGPcoder)**

### **“Deutschland sicher ins Netz” Initiative**

### **Vortrag über Cisco Sicherheit auf BlackHat Konferenz und Nachspiel...**

### **Mastercard Europay → GCMS mit Standort USA**

### **Phrack wurde eingestellt: So long and thanks for all the fish...**



## **Stichworte für 2006**

---

**Weiter steigende Unentspanntheit bei Hinweisen auf Sicherheitslücken**

**WarDriving usw. ist Out, WarFlying ist In (LH Flynet machts möglich)**

**Blackberry**

**P2P Würmer mit anständigen Schadensroutinen z.B. share \*.\***

**Firewall-Würmer**

**Die meisten Mobiltelefone können immer noch nicht vom User gepatched werden...**

- Wir warten also auf den MobileAlertCon / GSM Threat Level / ... Service

**TupperWare bringt "Tin-Foil-Hat" Taschen & Dosen in jeder Größe auf den Markt**

**Fussball-WM: mehr Kameras als Zuschauer ("Du bist Krimineller")**

**VoIP Spam? Mal sehen...**

**ELSTER und anders**

**Abwasserüberwachung zur Sicherung der nationalen Sicherheit?**





## ***Hinweise für 2006...***

---

**“When robbing bank, don't take your own laptop”**

**If you work for the US Navy, please remember to NOT**

**“use peer-to-peer (P2P) file sharing applications, such as Kazaa, Shareaza and OpenP2P without approval and only in support of Navy missions” !!1!**



## *Einen guten Rutsch..!*

---

```
Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

c:\>net user administrator Dein_neues_Password_höhö
The command completed successfully.

c:\>
```