pallas

eco Verband der deutschen Internetwirtschaft e.V.

Arbeitskreis Sicherheit

Veranstaltung:

Sitzung am 03. September 2008, Köln

Leitung:

Dr. Kurt Brand
Geschäftsführer Pallas GmbH

Pallas GmbH
Hermülheimer Straße 10
50321 Brühl

information(at)pallas.de
http://www.pallas.de

Agenda

eco - AK Sicherheit - 03.09.2008

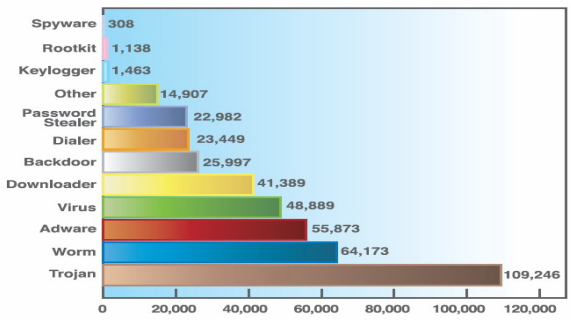
13:00	Registrierung
13:30	Begrüßung und Vorstellung
13:45	**Wie der CISO wirkt - Qualitative Wirkungsanalyse, Ergebnisse einer tiefenpsychologischen Studie** Dietmar Pokoyski known_sense
14:30	**Rechtliche Stellung des CISO** Jens Eckhardt JUCONOMY Rechtsanwälte
15:15	Kaffeepause & Networking
15:45	Aktuelle Lage im Sicherheitsbereich
16:00	Ziele und Themen des Arbeitskreises
16:45	Verschiedenes, nächster Termin
17:00	Ende der Veranstaltung

Agenda

eco - AK Sicherheit - 03.09.2008

13:00	Registrierung
13:30	Begrüßung und Vorstellung
13:45	Wie der CISO wirkt - Qualitative Wirkungsanalyse, Ergebnisse einer tiefenpsychologischen Studie Dietmar Pokoyski known_sense
14:30	Rechtliche Stellung des CISO Jens Eckhardt JUCONOMY Rechtsanwälte
15:15	Kaffeepause & Networking
15:45	**Aktuelle Lage im Sicherheitsbereich**
16:00	Ziele und Themen des Arbeitskreises
16:45	Verschiedenes, nächster Termin
17:00	Ende der Veranstaltung

Neue Malware 2007, Gesamtanzahl

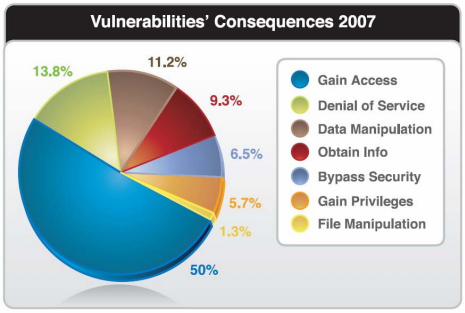


zitiert nach IBM Internet Security Systems X-Force 2007 Trend Statistics

- Trend zu hochentwickelten und zielgenauen Trojanern sowie tagesaktuellen Angriffen (1. April, Erdbeben, Olympiade, …)
- Trend zu Blended Threats (z.B. Email-Web-Angriffe), Websense: 3/4 aller Emails enthalten Link auf Mal/Spam-Sites
  (State of Internet Security, Q1 - Q2, 2008)

SW-Sicherheitslücken 2007

Vendor	Vulnerabilities Reported in 2007
Microsoft	238
Apple	207
Oracle	183
IBM	137
Cisco	113

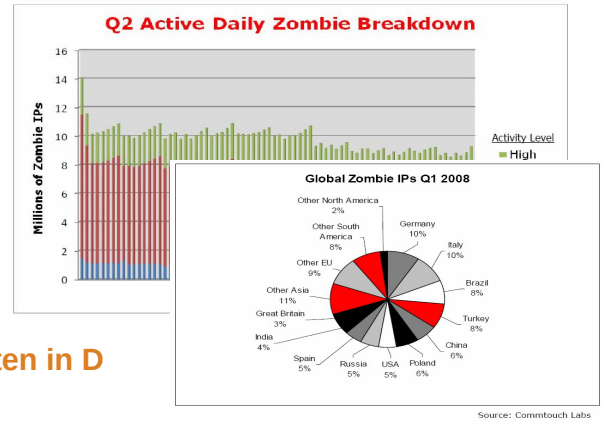


- Anzahl Patches in 2007 für kritische Sicherheitslücken:
  Internet Explorer: 28
  Firefox: 36

zitiert nach IBM Internet Security Systems X-Force 2007 Trend Statistics

Gain Access: Make Zombies

- Größte Bedrohung derzeit durch **Botnetze**: verseuchte Rechner, illegal ferngesteuert **(Zombies)**; senden Spam (85 %), Viren (100 %), Phishing-, Denial-of-Service-Attacken
- Botnetze können 1 Mio PCs umfassen; täglich mehrere Hunderttausend neue Zombies; **1/4 aller PCs verseucht**

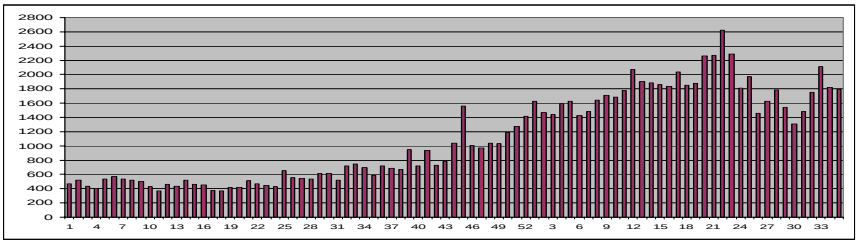


- **Q1/2008: die meisten in D**

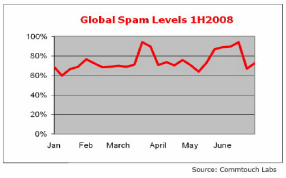
zitiert nach Commtouch

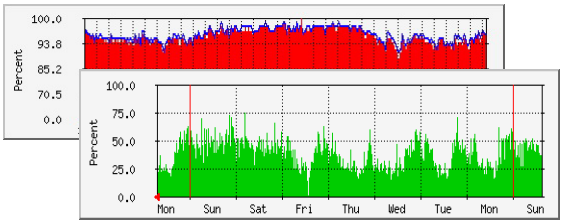
Spam Anfang 2007 bis heute: Starkes Wachstum

- Wochenend-Spam in Pallas-Honeypot Jan 07 – Aug 08



- **Spamquote 93 %**
  (Pallas, August 2008)



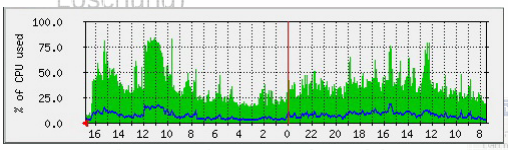


Global: 77 %
(Commtouch)

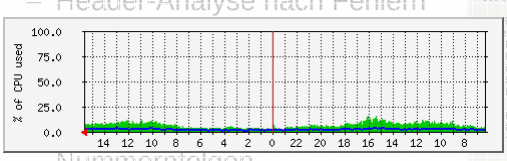
Zum Vergleich: Spamquote 2004 bei Pallas

Klassische Spam-Filter überfordert

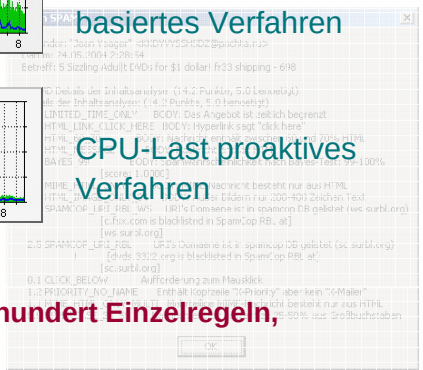
- Vorverarbeitung
  - Festlegung der Verarbeitung nach Empfänger (Log, Markierung, Löschung)
- Header-Analyse nach Fehlern
- Nummernfolgen
- „Schreiender“ Text



CPU-Last content-basiertes Verfahren



CPU-Last proaktives Verfahren

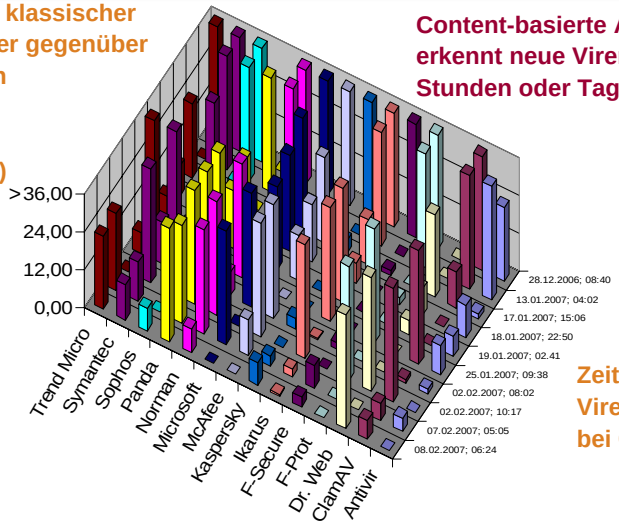


Content-basierte Arbeitsweise, viele hundert Einzelregeln, sehr hohe Ressourcenbelastung!

Klassische Malware-Filter überfordert

Verspätung klassischer Virenscanner gegenüber Commtouch Zero-Hour Protection (in Stunden)

Content-basierte Arbeitsweise, erkennt neue Viren erst nach Stunden oder Tagen!

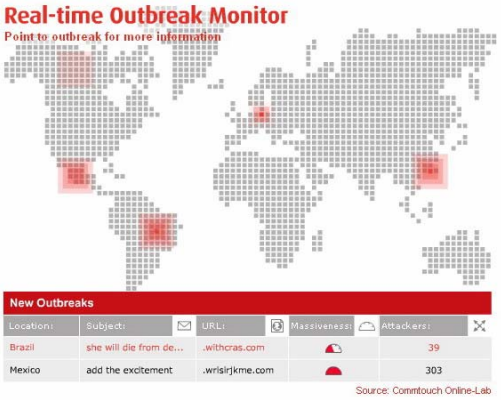


Zeit der Virenerkennung bei Commtouch

Informationen aus Commtouch Virus Outbreak Reports, 01.01.2007-14.02.2007

Abwehr durch proaktive Real-Time-Verfahren, z.B.

- **Zero-Hour Protection (ZHP)** gegen Viren und andere Malware
- **Real-Time Anti-Spam (RTAS)** gegen Spam
- **GlobalView IP-Reputation** gegen Zombies u. a. Müllversender



Gerne beantworte
ich Ihre Fragen

pallas

Dr. Kurt Brand
Pallas GmbH
Hermülheimer Straße 10
50321 Brühl

info (at) pallas.de
http://www.pallas.de