pallas

eco Verband der deutschen Internetwirtschaft e.V.

Arbeitskreis Sicherheit

Veranstaltung:

Sitzung am 04. Februar 2009, Frankfurt

Thema: Botnetze

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 - 04.02.2009: Botnetze

13:00	Registrierung
13:15	Begrüßung
13:30	**Bots im Kontext von Spam** Christian J. Dietrich, Institut für Internet-Sicherheit
14:10	**Tracking Botnets** Thorsten Holz, Universität Mannheim
14:50	**Projekte des LKA Nieders. z. Bekämpfung v. Botnetzen** Jens Kolpack, LKA Niedersachsen
15:30	Kaffeepause & Networking
16:00	**Abuse-Management bei NetCologne - ... Zombies** Dietmar Braun, Gunther Nitzsche, NetCologne GmbH
16:40	**Rechtliche Aspekte...Botnetze -...Strategie eco BKA BSI** RA Frank Ackermann, eco
17:10	**Aktuelle Lage im Sicherheitsbereich: Zombies und mehr** Dr. Kurt Brand, Pallas GmbH
17:40	Verschiedenes, Themen und Termine
18:00	Ende der Veranstaltung

pallas

Aktuelle Lage im Sicherheitsbereich:

Zombies und mehr

Veranstaltung:

Sitzung am 04. Februar 2009, Frankfurt
Thema: Botnetze

Referent:

Dr. Kurt Brand
Geschäftsführer Pallas GmbH

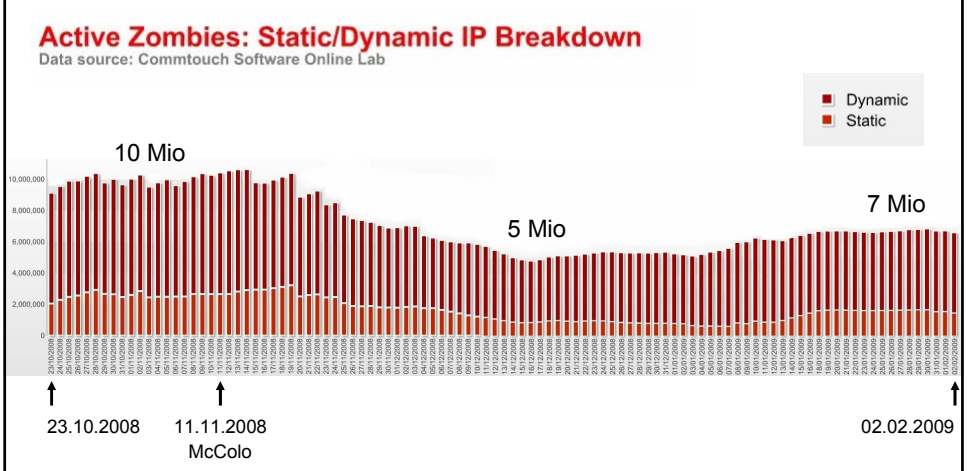
Pallas GmbH
Hermülheimer Straße 10
50321 Brühl

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

Hack von Verkehrsschildern, USA, 01/2009

© Spiegel Online, 30.01.2009

Anzahl täglich beobachteter Zombies



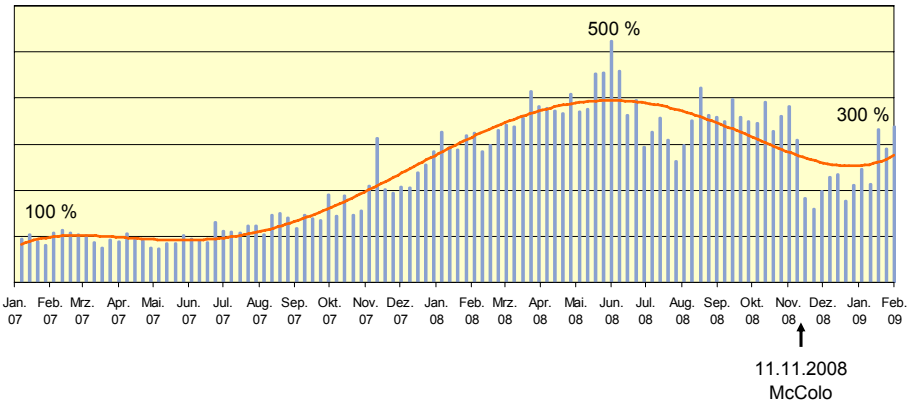
© **Commtouch**
www.commtouch.com

Abwehr: Real-time Sender Reputation

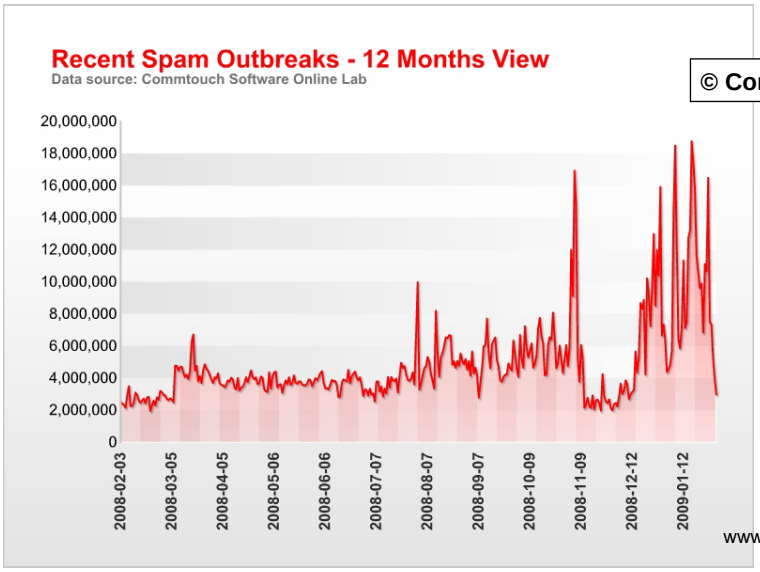
Ermittlung: Web-Interface Pallas/Commtouch

2 Jahre Spamzählung bei Pallas

Spam um ein Jahr "zurückgeworfen"



Anzahl Spam-Ausbrüche signifikant gewachsen



Größerer Malware-Ausbruch 01.12.2008: Oft kein Real-Time-Schutz

MD5 checksum:	e43447e6889fcc9c66a1756854d08441
Commtouch detect time [GMT]:	12/2/2008 12:24:00 AM
Parent archive files(s):	hinweis.zip, sperrung.zip
File name(s):	sperrung.exe

Comparative Data

This report generated 33:41 hrs. after Commtouch detect time

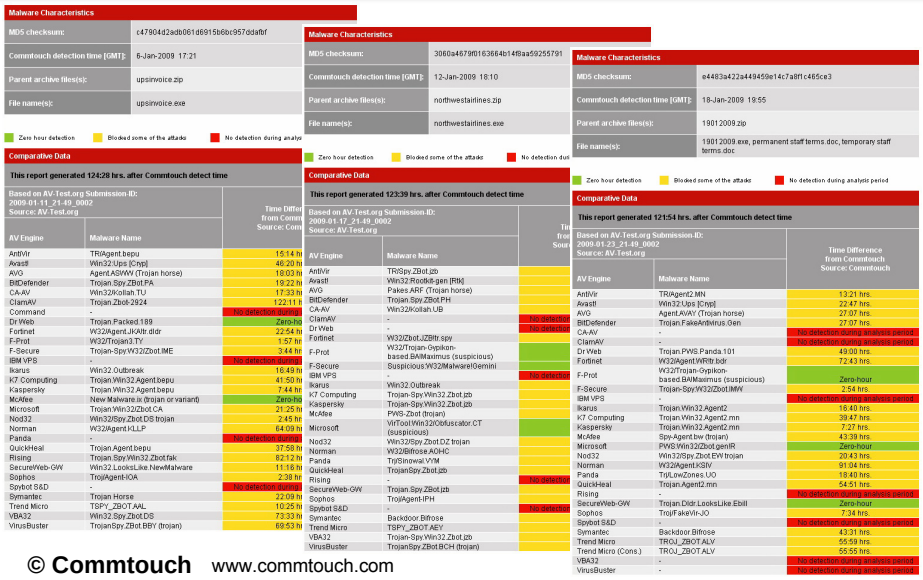
Based on AV-Test.org Submission-ID: 2008-12-03_10-05_0005 Source: AV-Test.org		Time Difference From Commtouch Source: Commtouch Software, Ltd.
AV Engine	**Malware Name**	
AntiVir	TR/Dldr.iBill.BV	Zero-hour
Avast!	Win32:Downloader-CCA [Trj]	10:41 hrs.
AVG	Agent.ANJC (Trojan horse)	Zero-hour
BitDefender	Trojan.FakeAlert.APY	Zero-hour
CA-AV	Win32/SillyDl.GEK	23:42 hrs.
ClamAV	Trojan.Downloader-60790	Zero-hour
Command	W32/Trojan3.MX (destructive program)	0:23 hrs.
Dr Web	-	No detection during analysis period
Fortinet	W32/Emold.C!tr	1:21 hrs.
F-Prot	W32/Trojan3.MX	Zero-hour
F-Secure	Trojan-Downloader:W32/Agent.IDO	Zero-hour
IBM VPS	-	No detection during analysis period
Ikarus	Win32.Outbreak	Zero-hour
K7 Computing	-	No detection during analysis period
Kaspersky	Trojan-Dropper.Win32.Agent.aara	15:11 hrs.
McAfee	Spy-Agent.bw (trojan)	18:29 hrs.
Microsoft	VirTool:Win32/Obfuscator.CT (suspicious)	Zero-hour
Nod32	Win32/AutoRun.FakeAlert.AH worm	Zero-hour
Norman	-	No detection during analysis period
Panda	Trj/Agent.LAJ	20:28 hrs.
QuickHeal	-	No detection during analysis period
Rising	Trojan.Win32.Emold.d	8:50 hrs.
SecureWeb-GW	Trojan.Dldr.iBill.BV	Zero-hour
Sophos	Troj/Mdrop-BXF	Zero-hour
Spybot S&D	-	No detection during analysis period
Symantec	W32.Auraax	15:36 hrs.
Trend Micro	TROJ_MULDROP.AB	4:10 hrs.
VBA32	-	No detection during analysis period
VirusBuster	Worm.DR.Autorun.CBT (trojan)	19:01 hrs.

Verspätung gegenüber Commtouch Zero Hour Protection

Zeiten ermittelt von AV-Test.org

© Commtouch
www.commtouch.com

Ausbrüche im Januar 2009



© **Commtouch** www.commtouch.com

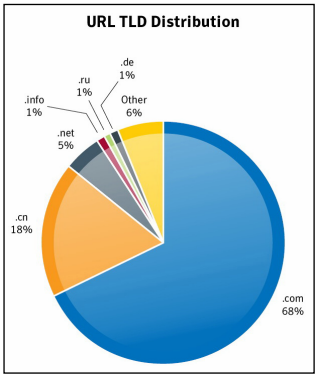
Die Lage: Was war – was wird?

WAR

- MSRT hat in 11/08 1 Mio PCs von Scare-Ware bereinigt
- McAfee beziffert weltweiten Schaden durch Internet-Kriminalität auf 1.000.000.000.000 $
- Confickr auf Kriegsschiffen der Royal Navy?
- Größter Klau von Kreditkartendaten (Meldg. 01/09)

WIRD

- Mehr verseuchte Websites (Drive-by)
  90 % der Spams mit URL (Symantec, 01/09)
  77 % Malpages: seriös (Websense , 01/09)
- Real-Time URL-Filter!
- Nutzung personenbezogener Daten aus Social Networks → MySpam?
- Kostenl. AV von MS Mitte 09? "Morro" (privat)
- DNSSEC ?



© Symantec

Verschiedenes, Termine und Themen

- 3 Regeltermine pro Jahr: erster Mittwoch 02 / 05 / 10
  nächste also 06.05.09 und 07.10.09
  ggf. weitere Treffen nach Bedarf
- Thema am 06.05.2009 in Köln
  IT-Sicherheit im Gesundheitswesen / Telemedizin
- 07.10.09: Thema und Pate gesucht
- Weitere interessante eco-Termine
  - 25.02.09: WS Anti-Spam-Maßnahmen, Köln,
    Moderator: D. Braun, NetCologne
  - 24.03.09: Saas und Cloud Computing
  - 31.03.09: Kongress Datenschutz eco + MMR

Gerne beantworte
ich Ihre Fragen

pallas

Dr. Kurt Brand
Pallas GmbH
Hermülheimer Straße 10
50321 Brühl

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