



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



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



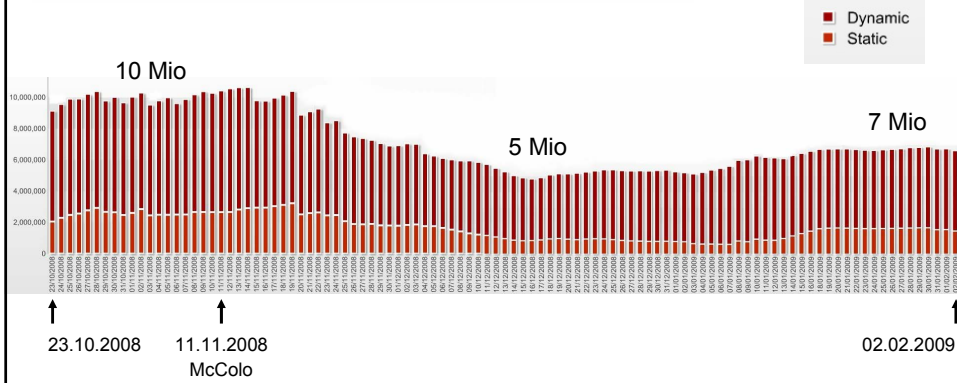
© Spiegel Online,
30.01.2009

Anzahl täglich beobachteter Zombies



Active Zombies: Static/Dynamic IP Breakdown

Data source: Commtouch Software Online Lab



© Commtouch
www.commtouch.com

Abwehr: Real-time Sender Reputation

Ermittlung: Web-Interface Pallas/Commtouch

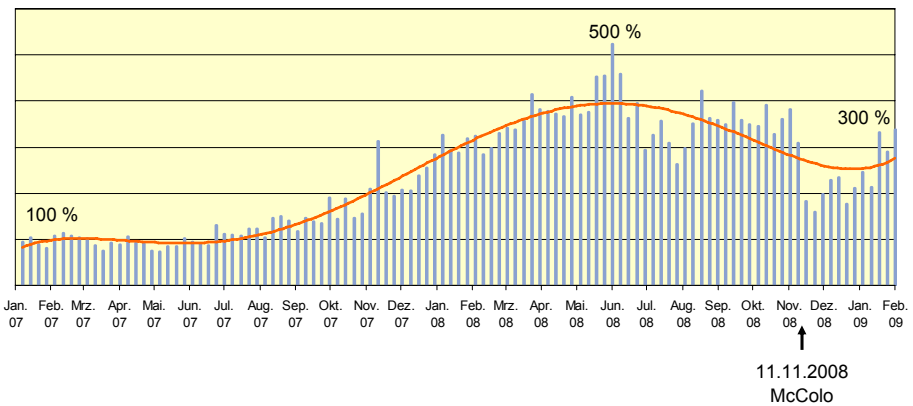
eco AK Sicherheit - 04.02.2009

© Pallas GmbH. Alle Rechte vorbehalten.

2 Jahre Spamszählung bei Pallas



Spam um ein Jahr "zurückgeworfen"



eco AK Sicherheit - 04.02.2009

© Pallas GmbH. Alle Rechte vorbehalten.

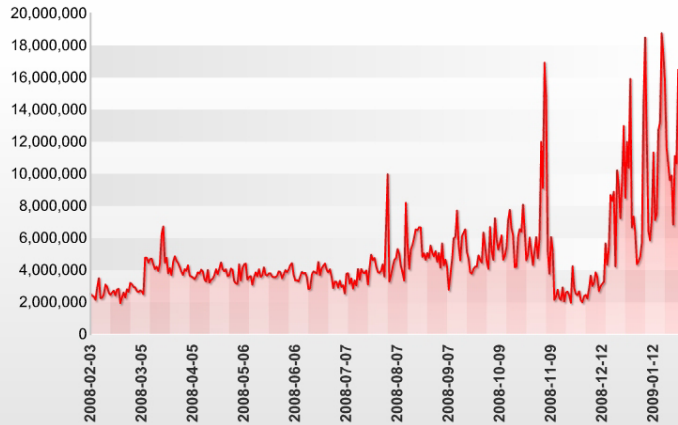
Anzahl Spam-Ausbrüche signifikant gewachsen



Recent Spam Outbreaks - 12 Months View

Data source: Commtouch Software Online Lab

© Commtouch



www.commtouch.com

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



AV Engine	Malware Name	Time Difference From Commtouch
AntiVir	TR/Dir.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-AM	Win32/Silly.DI.GEK	23:42 hrs.
ClamAV	Trojan.Downloader-50790	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.Didr.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



Malware Characteristics		Malware Characteristics		Malware Characteristics	
MDS checksum:	c478042ad0601d691560be9570dafb	MDS checksum:	308046790163664b146aa59255791	MDS checksum:	e4482a4224448492e14c7a0ff1c456c3
Command detection time (GMT):	6-Jan-2009 17:21	Command detection time (GMT):	12-Jan-2009 16:10	Command detection time (GMT):	18-Jan-2009 18:55
Parent archive file(s):	upsrvoice.zip	Parent archive file(s):	northwestairlines.zip	Parent archive file(s):	19012009.zip
File name(s):	upsrvoice.exe	File name(s):	northwestairlines.exe	File name(s):	19012009.exe, permanent staff terms.doc, temporary staff terms.doc
<input type="checkbox"/> Zero hour detection <input type="checkbox"/> Blocked some of the attacks <input type="checkbox"/> No detection during analysis		<input type="checkbox"/> Zero hour detection <input type="checkbox"/> Blocked some of the attacks <input type="checkbox"/> No detection during analysis		<input type="checkbox"/> Zero hour detection <input type="checkbox"/> Blocked some of the attacks <input type="checkbox"/> No detection during analysis period	
Comparative Data This report generated 124226 hrs. after Commtouch detect time		Comparative Data This report generated 123339 hrs. after Commtouch detect time		Comparative Data This report generated 121541 hrs. after Commtouch detect time	
Based on AV-Test.org Submission ID: 2009-01-23-09_0902 Source: AV-Test.org		Based on AV-Test.org Submission ID: 2009-01-23-09_0902 Source: AV-Test.org		Based on AV-Test.org Submission ID: 2009-01-23-09_0902 Source: AV-Test.org	
AV Engine	Malware Name	Time Diff. from Commtouch Source: Commtouch	AV Engine	Malware Name	Time Difference from Commtouch Source: Commtouch
AdVir	TRAgent.bapu	15.14 h	AdVir	TRSpy_ZBot.Lb	-
Avast	Win32/Upss [Cryp]	46.20 h	Avast	Win32/Frodoe-gen [RM]	-
AVO	Agent.ASW (Trojan horse)	18.02 h	AVO	Pakes ARF (Trojan horse)	-
BitDefender	Trojan.Spy.ZBot.PA	19.22 h	BitDefender	Trojan.Spy.ZBot.PH	-
CA-AY	Win32/Kolan.TU	11.33 h	CA-AY	Win32/Kolan.LB	-
ClanAV	Trojan.ZBot.2924	122.11 h	ClanAV	-	No detection
Command	-	-	Command	-	-
Dr.Web	Trojan.Fatched.189	299.30 h	Dr.Web	-	No detection
Fortinet	W32/Agent.AWid.dor	22.44 h	Fortinet	W32/Zbot.ZBIR.spy	-
F-Prot	W32/Trojan3.TY	1.57 h	F-Prot	W32/Trojan-Optikon-based.BAMainmus (suspicious)	-
F-Secure	Trojan.Spy.W32.ZBot.MC	3.48 h	F-Secure	Suspicious.W32/Mahesra09emini	-
IBM VPS	-	-	IBM VPS	-	No detection
Ikarus	Win32.Outbreak	16.43 h	Ikarus	Win32.Outbreak	-
KT Computing	Trojan.Win32.Agent.bapu	41.20 h	KT Computing	Trojan.Spy.Win32.ZBot.Lb	-
Kaspersky	Win32.Agent.bapu	7.44 h	Kaspersky	Trojan.Spy.Win32.ZBot.Lb	-
McAfee	New.Malware.A (Trojan or variant)	289.26 h	McAfee	FW32.Zbot (trojan)	-
Microsoft	Trojan.Win32.ZBot.CA	21.25 h	Microsoft	VirTool.Win32/Oousabor.CT (suspicious)	-
Nod32	Win32/Spy.ZBot.DS.trojan	2.45 h	Nod32	No32	-
Norman	W32/Agent.LLP	84.00 h	Norman	Win32/Spy.ZBot.DZ.trojan	-
Panda	-	-	Panda	W32/Bfrose.AQH.C	-
QuickHeal	Trojan.Agent.bapu	37.52 h	QuickHeal	Trojan.Spy.ZBot.Lb	-
Rising	Trojan.Spy.Win32.ZBot.fak	82.12 h	Rising	Trojan.Spy.ZBot.Lb	-
SecureWeb-GW	Win32.LooksLike.NemMalware	11.18 h	SecureWeb-GW	Trojan.Agent.PH	-
Sophos	Trojan.Agent.CA	2.20 h	Sophos	-	No detection
Spybot S&D	-	-	Spybot S&D	-	-
Symantec	Trojan horse	22.09 h	Symantec	Backdoor.Bfrose	-
Trend Micro	TSpy_ZBOT.ALV	10.25 h	Trend Micro	TROU_ZBOT.ALV	-
VBA32	Win32.Spy.ZBot.DS	73.33 h	VBA32	Trojan.Spy.Win32.ZBot.Lb	-
VirusBuster	Trojan.Spy.ZBot.MB (trojan)	89.53 h	VirusBuster	Trojan.Spy.ZBot.BCH (trojan)	-

© Commtouch www.commtouch.com

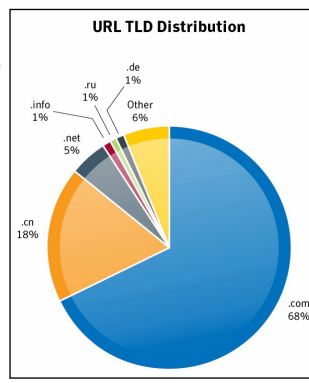
Die Lage: Was war – was wird?



WAR

WIRD

- 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 \$
- Conficker auf Kriegsschiffen der Royal Navy?
- Größter Klau von Kreditkartendaten (Meldg. 01/09)
- Mehr versuchte 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

eco AK Sicherheit - 04.02.2009

© Pallas GmbH. Alle Rechte vorbehalten.



Gerne beantworte
ich Ihre Fragen



Dr. Kurt Brand
Pallas GmbH
Hermülheimer Straße 10
50321 Brühl

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