VIRUS oder FEHLALARM?

Verwirrende Virenwarnungen: Hinter welchen Meldungen stecken echte Gefahren, welche sind harmlos? So finden Sie es heraus

VON CLAUDIO MÜLLER

Vertrauen Sie den Websites, die Sie regelmäßig besuchen? Malware-Entwickler hoffen darauf, denn zeigt der Browser auf einer bekannten Seite eine Warnung an, glaubt kaum ein User an einen Virus – und ignoriert die Warnung. Dass dieses Vertrauen gefährlich ist, zeigen Angriffe auf renommierte Seiten, wie zuletzt im April. Rund 500.000 Websites wurden Opfer einer Attacke, die gefährlichen Schadcode in die Seiten einschleuste – darunter auch einige Podcasts auf iTunes.

Auch in anderen Fällen setzen die Malware-Entwickler gezielt auf die Arglosigkeit der User. Neben dem Dauerbrenner Phishing-Mail konzentrieren sich Angreifer zurzeit besonders auf zwei Wachstumsmärkte: soziale Netzwerke und Smartphone-Apps. Noch immer glauben nur wenige User, dass Postings ihrer Facebook-Freunde gefährlich sein können. Doch täglich tauchen neue Attacken auf, die es auf die persönlichen Daten der User abgesehen haben. Und auch die Zahl der Apps im App-Store und besonders im Android Market, die Handydaten ausspähen oder User abzocken, nimmt rasant zu.

Andererseits konfrontieren Browser und Betriebssystem den User immer wieder mit eigentlich harmlosen Warnungen, hinter denen mancher einen Virenbefall vermutet: Geblockte Websites, Fehlalarme des Virenscanners, Windows-Meldungen. Die Unterscheidung, wo tatsächlich ein Virus lauert und wo nicht, ist schwierig. Wer an den richtigen Stellen und mit den passenden Tools sucht, findet die Lösung aber schnell.

Echter Virus: So tarnen sich Malware und Abzocker

GEHACKTE WEBSITES Angreifer nutzen vermehrt seriöse Seiten, um Malware zu verbreiten. Jüngstes Beispiel: Der erwähnte Angriff auf rund eine halbe Million Websites, der als LizaMoon-Attacke bekannt wurde. Per SQL Mass Injection haben Hacker Code in die Seiten eingefügt, der automatisch zu einer Seite weiterleitete, die die Malware gehostet hat. Die meisten dieser Weiterleitungen führten zur Domain lizamoon.com – daher der Name. Eine ähnliche Attacke er-

wischte im Juni letzten Jahres etwa 114.000 Seiten. Genau wie damals visierte der Liza-Moon-Angriff Seiten an, welche die Microsoft-Server-Plattform IIS und die Content-Entwicklungstechnologie ASP.net nutzten. Die Malware-Pakete auf den Zielseiten der Redirects suchen dabei gezielt nach ungepatchten Lücken im Browser, den Plug-ins oder in Windows selbst. Oft sind das Trojaner, die Daten ausspionieren oder Rogueware-Programme (siehe unten).

► Selbst wenn der Browser oder der Virenscanner eine Warnung anzeigt, rechnen User auf bekannten Seiten selten mit einem Angriff. Man würde ihn auch kaum bemerken, da er meist im Hintergrund ausgeführt wird. Daher sollten Sie immer den Virenscanner, den Browser und dessen Plug-ins aktualisieren, um Sicherheitslücken so gut wie möglich zu stopfen. Mit dem Firefox-Add-on NoScript regeln Sie zudem die Ausführung aktiver Elemente und blockieren eingebettete Skripte. Manchmal ist aber nicht die Seite selbst das Problem, sondern per iFrame auf der Seite eingefügte Inhalte. Gehen Sie daher nach der Installation von NoScript über das Icon neben der URL-Zeile zu »Einstellungen | Eingebettete Objekte« und aktivieren Sie dort die Funktion »<IFRAME> verbieten«.

FALSCHE VIRENFUNDE Warnungen des Windows Stability Centers sollte man ernst nehmen – oder? Lieber nicht, denn das Tool ist ein falsches Sicherheitsprogramm (Rogueware), das Sie mit gefälschten Warnungen abzocken will. Deren Ursprung liegt meist auf Websites, die zunächst per JavaScript-Skript eine echt wirkende Virenwarnung im Browser generieren. Klickt man dabei auf »Viren entfernen« oder ähnliche Buttons, startet der Download eines falschen und oft nur schwer zu entfernenden Virenscanners – zum Beispiel das Windows Stability Center. Auch das zeigt wieder falsche Ergebnisse an und bietet dem User nun die Lösung: eine kostenpflichtige, aber natürlich völlig nutzlose Pro-Version.

AUF DVD

Neben der Vollversion BitDefender Total Security 2011 finden Sie im Virencheckpaket unter dem CHIP-Code Fehlalarm Tools zur Netzwerkanalyse, zum Browserschutz, einen speziellen Rogueware-Jäger und weitere Sicherheitstools

Diese Polizeiwarnung ist ein Abzocktrick

Mit einer seriös wirkenden BKA-Meldung versuchten Erpresser kürzlich, dem User Geld abzuknöpfen. Die Fälschung erkennen Sie nur an Details

► Kaufen Sie das Tool nicht. Auf den ersten Blick wirken die Warnungen bedrohlich, beim zweiten Hinsehen sollten Sie aber die ungewöhnlich vielen Virenfunde misstrauisch machen. Generell sollten Sie nur vertrauenswürdige, bekannte Antiviren-Programme installieren. Sehen Sie eine solche falsche Warnung, checken Sie Ihren Rechner gründlich durch. Mit dem Tool Remove Fake Antivirus (auf Heft-DVD) finden und entfernen Sie die häufigsten Exemplare.

VERSUCHTE ERPRESSUNG Die seit April kursierende angebliche Warnung vom Bundeskriminalamt BKA (siehe oben) behauptet, dass auf dem User-PC Kinderpornografie und terroristisches Material gefunden wurde. Dahinter steckt ein Trojaner, der jegliche Systemzugriffe blockiert. Erst nach Zahlung von 100 Euro würde der Rechner entsperrt werden. Der Erfolg solcher Erpresser-Software hängt davon ab, ob die User auf die angezeigte Warnung hereinfallen.

► Trotz Originallogos oder echt aussehender Windows-Meldungen kann man derartige Erpressungsversuche erkennen. Seltsame Geschäftspraktiken (Windows-Aktivierung ausschließlich über ausländische Telefonnummern), Rechtschreibfehler, Mailadressen, die nicht auf eine offizielle Domain verweisen, oder anonyme Bezahlverfahren deuten auf den Schwindel hin. Aber selbst wer nicht bezahlt, muss den Rechner noch desinfizieren. Da die Systemzugriffe in Windows meist komplett gesperrt sind, helfen nur ein Neustart und ein Systemcheck mit der Live-CD des Antivirenprogramms. Bringt auch das nichts, bleibt nur eine Neuinstallation von Windows.

VERFÜHRERISCHE FACEBOOK-LINKS Auf Facebook verbreiten sich betrügerische Inhalte rasend schnell. Der Grund: Viele User klicken leichtfertig auf Inhalte, die angeblich von ihren Freunden kommen. Die harmlose Variante dieses sogenannten Facebook- →

Scam sind Videos, die Promi-Sensationen, Gewalt oder Sex versprechen. Klickt man auf einen solchen Videolink, werden die Inhalte über einen verborgenen „Gefällt mir"-Button im Userprofil gepostet. Dahinter stecken oft Werbefirmen, die mit jedem Klick Geld verdienen. Gefährlicher jedoch sind Apps, die etwa versprechen, dass Sie Ihre Profilbesucher sehen können – was auf Facebook nicht möglich ist. Solche Apps geben die Userdaten unerlaubt weiter oder klauen sogar Passwörter und infizieren den Rechner mit Malware.

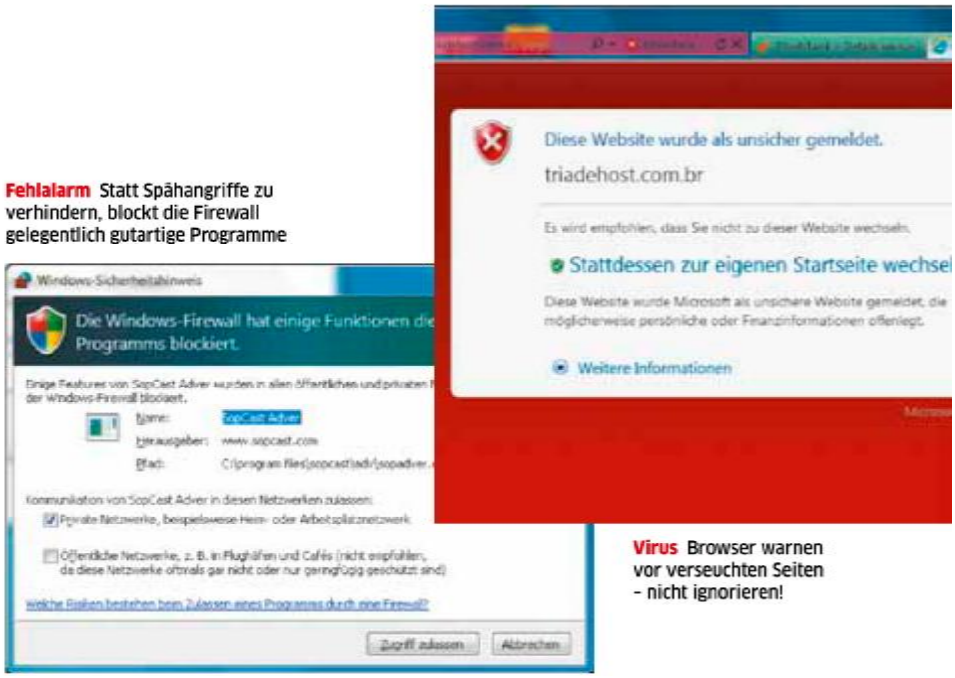
► An seltsamen Links wie chalaepic.zapto.org können Sie die unseriösen Videos schnell identifizieren. Bei Apps sollten Sie genau darauf achten, welche Daten sie nutzen. Bereits zugelassene Apps entfernen Sie unter »Konto | Privatsphäre-Einstellungen | Anwendungen und Websites | Bearbeite deine Einstellungen«. Zur Sicherheit sollten Sie auch nach jeder Scam-Attacke ein neues Passwort festlegen. Dies tun Sie unter »Konto Kontoeinstellungen Passwort | ändern«.

ABZOCK-APPS FÜRS SMARTPHONE Die Anwendungen in den App-Stores für iOS oder Android sind nicht immer so harmlos, wie sie aussehen. Besonders bei Gratis-Apps kann es passieren, dass Sie per Klick auf ein Werbebanner unbemerkt ein Abo abschließen, das automatisch über Ihre Mobilfunkrechnung abgerechnet wird. Noch fieser sind Smartphone-Viren. Im März haben Hacker mehr als 50 Android-Apps mit der Malware DroidDream infiziert, unter anderem Photo Editor, Super Guitar Solo und Best password safe. In vier Tagen wurden die Apps laut Panda 50.000-mal heruntergeladen. Einmal installiert, können solche Viren die Daten auslesen, teure SMS automatisch verschicken oder Administratorrechte freischalten und damit weitere Malware laden.

► Virenschutz-Apps fürs Smartphone verhindern solche Attacken. Eine schlanke und effektive Lösung ist AVG Anti-Virus Free (gratis im Android Market). Nach der Installation einer App sollten Sie zudem in den Anwendungsinfos überprüfen, ob sie auf Ihre Nachrichten oder Browserhistory zugreift – das ist typisch für Abzocker und Spione. Finden Sie auf der Rechnung doch einmal ungewöhnliche Posten, beanstanden Sie dies beim Provider. Allerdings müssen Sie auf Kulanz hoffen, da Sie kaum beweisen können, dass Sie ungewollt ein Abo abgeschlossen haben.

PROFESSIONELLES PHISHING Per Mail verbreitete Phishingseiten nehmen wieder zu: Allein von Januar zu Februar stieg die Zahl der Phishing-Mails laut Symantec um 50 Prozent. Die Mails verlinken zu professionell nachgebauten Banking-Seiten, auf denen Sie Ihre Log-in-Daten eingeben sollen.

► Geben Sie die Webadressen der Banken, Shops oder Bezahldienste immer manuell ein oder rufen Sie sie über Bookmarks auf – und bedenken Sie, dass Banken nie solche Mails verschicken. Achten Sie bei Banken und Bezahldienstseiten darauf, ob sie https-Verbindungen nutzen, nur dann sind sie sicher. Auch ungewöhnliche Domains wie paypaldeb.com sind verdächtig. Klicken Sie dort andere Links oder Unterseiten an, funktionieren diese meist nicht. Wenn Sie bei der Eingabe von Zugangsdaten eine Fehlermeldung erhalten und es erneut versuchen sollen, kann auch das ein Trick sein. Angreifer wollen damit auch Zweitkonten abzocken.



Fehlalarm Statt Spähangriffe zu verhindern, blockt die Firewall gelegentlich gutartige Programme

Virus Browser warnen vor verseuchten Seiten – nicht ignorieren!

Fehlalarm: So verunsichern harmlose Meldungen

AGGRESSIVE VIRENSCANNER Wenn der eigene Virenscanner eine Warnung ausspuckt, sollte man diese ernst nehmen. Leider kommt es aber gelegentlich zu Fehlalarmen, wenn Sie eine Anwendung installieren oder ausführen (siehe Tabelle unten). Zwar sind die Zahlen der Fehlalarme Anfang dieses

So oft nerven Security Suiten mit falschen Warnungen

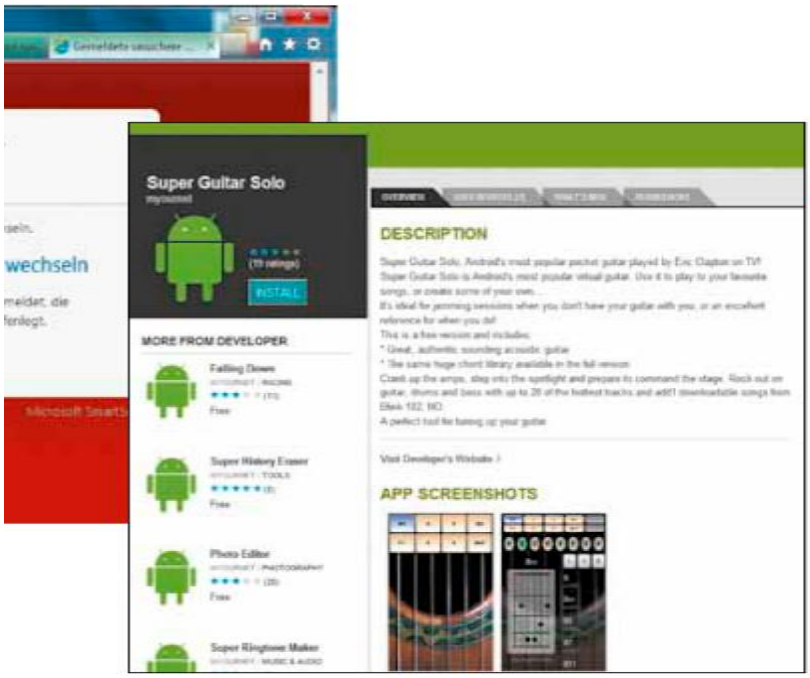
Während zu scharf eingestellte Scanner wie von Avira oder McAfee häufig Fehlalarm schlagen, verunsichern die Programme von Avast oder Microsoft den User nur selten

FEHLALARME

Anbieter	Avast Free Antivirus 5	AVG Internet Security 10	Avira Premium Security Suite 10	Bitdefender Internet Security Suite 2011	Bullguard Internet Security 10	Comodo Internet Security Premium 5	Eset Smart Security 4.2	F-Secure Internet Security 2011	G Data Internet Security 2011	Kaspersky Internet Security 2011	McAfee Total Protection 2011	Microsoft Security Essentials 2	Escan Internet Security Suite 11	Norman Security Suite Pro 8	Panda Internet Security 2011	PC Tools Internet Security 2011	Sunbelt Vipre Antivirus Premium 4	Norton Internet Security 2011	Trend Micro Titanium Internet Sec. 2011	Webroot Internet Security Complete 7
Systemscan: Fehlalarme [1]	1	8	8	5	7	25	9	7	8	11	31	1	9	39	9	7	24	17	7	15
Echtzeit-Wächter: Warnungen/ Blockierungen [2]	0/0	1/0	7/1	0/0	0 / 0	1/3	0/0	0/0	0/0	1/1	3/0	0/0	0/1	0/0	1/0	6/0	0/0	0/0	0/0	2/4

QUELLE: AV-TEST

[1] 841.767 Testdateien, Januar bis März 2011
[2] Warnungen bei Installation und Ausführung 20 typischer Anwendungsprogramme



Abzocke Hinter der harmlos wirkenden Musik-App steckt ein Datenspion

Jahres laut AV-Test im Vergleich zum vierten Quartal 2010 zurückgegangen. Aber immer noch meckern Security Suiten bei etlichen bekannten Anwendungen – selbst bei vollkommen harmlosen wie OpenOffice oder Notepad++. Schuld daran ist meist eine zu scharfe Heuristik, die bestimmte Codeteile oder Dateiaktionen in gutartigen Programmen als verdächtig einstuft. Ob eine Warnung angezeigt wird, hängt dabei von einem Schwellenwert ab. Wird der überschritten, schlägt der Scanner an.

► Wenn Sie das blockierte Programm kennen, sollten Sie mit einem Tool wie FileAlyzer die Prüfsumme der Set-up-Datei mit dem oft auf der Downloadseite des Anbieters angegebenen Wert abgleichen. Dies bietet sich vor allem bei großen Files, etwa dem Installer der Open-Office-Suite, an. Finden Sie auf der Website keine Prüfsumme, laden Sie das Programm zur Sicherheit noch einmal aus einer vertrauenswürdigen Quelle, etwa **chip.de**. Ist die blockierte Datei unbekannt, verschieben Sie sie in die Quarantäne und starten den Gegencheck. Laden Sie das File mit VirusTotal Uploader (auf Heft-DVD) hoch und lassen Sie es von über 40 Engines analysieren. Wenn nur ein oder zwei anschlagen, ist es wohl keine Malware.

GEBLOCKTE INTERNETANGEBOTE Die Phishingfilter der Browser basieren auf Blacklists, die Schadcode verbreitende URLs enthalten. Diese Listen sind überwiegend zuverlässig und blocken die gefährlichen Seiten, sind aber nicht immer topaktuell. Ständig gehen neue Schadseiten ins Netz, die Zahl hat sich im letzten Jahr auf knapp 3.300 pro Tag verdoppelt. Manchmal ist jedoch nicht die Seite selbst verseucht, sondern nur eines der Werbebanner. Das infizierte Banner wird zwar meist schnell entfernt, aber steht die Seite erst mal auf der Blacklist, blockiert der Browser sie noch tagelang.

► Checken Sie die geblockte URL mit dem Webpage Scanner von AVG (**avgthreatlabs.com/sitereports**), der die URL inklusive Subdomains in Echtzeit analysiert. Vor infizierten Bannern können Sie sich auch mit einem Adblocker für den Browser schützen.

FALSCHE ZERTIFIKATE SSL-verschlüsselte Websites benötigen Zertifikate, damit der Browser ihre Echtheit verifizieren und sie von unseriösen oder gefährlichen Seiten unterscheiden kann. Sind die Zertifikate nicht im Browser hinterlegt, blockiert er die Seite und zeigt dem User eine Warnung an.

► Diese Warnungen können ganz harmlose Ursachen haben: Ein falsch eingestelltes Datum im System (Windows oder BIOS), ein tatsächlich abgelaufenes Zertifikat (eher selten) oder ein Zertifikat von unbekannter Herkunft. Dies gilt etwa für einige kostenlose Zertifikate, wie die von CAcert, die Sie dann über ein Auswahlfenster im Browser direkt herunterladen und dort hinterlegen können. Aktuelle Browser sind dabei so streng, dass Sie diese Zertifikat-Warnungen nicht einfach wegklicken können.

NERVIGE WINDOWS-UAC Die Windows-Benutzerkontensteuerung (UAC) unterscheidet nicht zwischen Malware und gutartiger Software. Sie warnt standardmäßig immer, wenn eine Anwendung die Windows-Einstellungen (etwa die Registry) verändern will. Das dabei aufpoppende Fenster klicken erfahrene PC-User meist ungelesen weg, unerfahrene User sind eher verunsichert.

► Unter »Systemsteuerung | System und Sicherheit | Wartungscenter | Einstellungen der Benutzerkontensteuerung ändern« können Sie die Schärfe der UAC verringern. Wenn Sie sie ganz deaktivieren, sollten Sie Windows aber nicht mit Admin-Rechten nutzen, da Malware sonst leicht ins System gelangen kann. Richten Sie daher einen schnellen Benutzerwechsel ein, mit dem Sie per Klick die Admin-Rechte aktivieren, etwa um Tools zu installieren. Wie das geht, erfahren Sie im PDF „Sicher per Knopfdruck" auf der Heft-DVD.

ÜBEREIFRIGE FIREWALL Nicht jedes Programm, das Daten ins Web sendet, ist ein Trojaner, der Ihre Konto-, Kreditkarten- oder Log-in-Daten abgreift. Auch einige gutartige Programme senden Daten ins Web. Bei Browsern schlägt die Firewall nicht an, P2P-TV-Tools wie TVU oder SopCast, die andere Ports zur Datenübertragung nutzen, werden schon mal blockiert.

► Sind Sie unsicher, können Sie mit CurrPorts (auf Heft-DVD) aktive Netzwerkverbindungen analysieren. Blenden Sie dabei alle Systemprozesse aus, indem Sie in »Options« die Funktion »Display Items without Remote Address« deaktivieren. Übrig bleiben sollten nur Ihnen bekannte Programme. Sehen Sie einen anderen Prozess, finden Sie unter dem Reiter »Process Path« den Dateiort und laden das File von dort per VirusTotal Uploader zum Virencheck hoch. Bestätigt sich der Virenverdacht, trennen Sie in CurrPorts per [Strg]+[T] die Verbindung des belegten Ports und beenden den Prozess im Kontextmenü mit »Kill Processes of selected Ports«.

TYPISCHE SYSTEMFEHLER Schlecht programmierte Malware kann Abstürze oder Speicherfehler verursachen. Das ist aber eher selten, da sie im Verborgenen arbeitet. Zudem kursieren im Web viele bewährte Malware-Kits. Die Ursachen von Systemfehlern sind daher meist Konflikte im Speichersystem, alte Treiber oder Hardwareverschleiß.

► Checken Sie im Geräte-Manager, ob Hardwarekonflikte vorliegen, und aktualisieren Sie gegebenenfalls die Treiber. Speziell bei älteren Betriebssystemen (Windows XP oder dessen Vorgänger) kann das helfen, neuere Windows-Versionen laden die passenden Treiber im Normalfall automatisch herunter. Haben Sie vor dem Problem ein Programm installiert, rufen Sie per Systemwiederherstellung einen früheren Zustand auf, in dem der Rechner noch funktioniert hat. Befreien Sie mit CCleaner oder Defraggler von der Heft-DVD die Festplatte und Registry noch von Dateileichen sowie alten Einträgen, gehören Systemfehler der Vergangenheit an. So erhalten Sie auch keine Warnmeldungen mehr – zumindest bis die nächste Website gehackt wurde.

CLAUDIO.MUELLER@CHIP.DE