ZDF heute
ZDF heute journal
ZDF heute nacht

Service
- Podcast-Angebot
- heute-Telegramm
- Bildschirmschoner
- Mobile Dienste
- WAP-Dienste
- Newsletter
- RSS-Angebot
- Nachrichtenbanner
- Sidebar
- heute als Startseite

dpa, reuters, ZDF [M]

Terror-Spam meldet Anschlag in der Nachbarschaft

Neue Masche - Die meisten Schutzprogramme müssen passen

von Alfred Krüger und Volker Heil

Cyberkriminelle verbreiten ihre Schadprogramme mit perfiden Psycho-Tricks. Die jüngste Masche: Eine falsche Sensationsmeldung soll E-Mailempfänger auf eine manipulierte Nachrichtenwebseite locken: Eine Bombe sei explodiert - im Heimatort des Nutzers.

Drucken Versenden 24.03.2009 [Archiv]

"Warum musste das gerade bei euch passieren?" Das klingt wie ein entsetzter Aufschrei. Sophia scheint fassungslos. Offenbar hat sie gerade erst von dem furchtbaren Terroranschlag gehört. "In deiner Stadt wurden mindestens 18 Menschen getötet", schreibt sie in ihrer E-Mail. Der beigefügte Link verspricht erste Informationen. Er ist rasch angeklickt und öffnet eine Webseite, die auf den ersten Blick wie eine Seite der Nachrichtenagentur Reuters aussieht.

Spam der übelsten Sorte

Tatsächlich! Da steht es schwarz auf weiß: "Gewaltige Explosion erschüttert Göttingen... Mindestens zwölf Menschen starben, mehr als 40 wurden verletzt..." Die ersten Videobilder vom Ort des schrecklichen Anschlags sind nur einen Mausklick weit entfernt. Wer würde das Video nicht auf der Stelle anklicken?

Nachricht und Webseite sind gefälscht. Ebenso die E-Mail jener Dame, die sich Sophia, manchmal auch Irene nennt. Es handelt sich um Spam der übelsten Sorte. Die E-Mails sollen auf eine präparierte Webseite locken. Das Besondere an dieser Seite: Die gefälschten Schreckensmeldungen besitzen einen geografischen Bezug zum Mailempfänger. Sein Standort wird ermittelt und automatisch in die Meldung eingefügt - ein perfider Trick, durch den die Nachricht authentisch wirken soll.

Ortsnahe Meldung verunsichert Nutzer

Spammails dieser Art werden gegenwärtig massenhaft verbreitet. Sie sind in englischer Sprache abgefasst und sollen dafür sorgen, dass die Rechner argloser E-Mailnutzer mit einem Schadprogramm verseucht werden. Denn wer das Video auf der Webseite mit der angeblichen Schreckensmeldung anklickt, wird aufgefordert, umgehend eine neue Version des Flashplayers herunterzuladen und zu installieren. Ohne die neue Flashversion könne das Video nicht abgespielt werden.

Im Rechner wird natürlich keine neue Programmversion des Flashplayers, sondern eine Datei mit Namen wie "main.exe", "run.exe", "print.exe" oder "contact.exe" installiert. Viele Mailempfänger sind durch die ortsnahe Schreckensmeldung so verunsichert, dass sie alle Sicherheitsbedenken über Bord werfen und das angebotene Programm fraglos aktivieren. Dahinter verbirgt sich der Computerwurm Waledac, der seit Dezember 2008 im Internet sein Unwesen treibt und seine Opfer mit geschickt formulierten E-Mailtexten leimen will.

"Anklicken, drucken, sparen"

So verschickten die Waledac-Verbreiter zu Weihnachten gefälschte Benachrichtigungsmails über den Empfang einer elektronischen Postkarte mit Weihnachtsgrüßen. Dieselben Täter waren für die Spamfluten zum Valentinstag verantwortlich. Statt der angekündigten Liebesgrüße holte sich der Nutzer Mitte Februar den Waledac-Wurm in seinen Rechner.

Kurz danach sorgte eine weitere Spammail-Kampagne für eine Vielzahl infizierter Rechner. Die Waledac-Verbreiter nutzten die aktuelle Wirtschaftskrise und versprachen in ihren Lock-E-Mails Coupons mit Sonderrabatten für diverse Einzelhandelsgeschäfte in der näheren Umgebung des Empfängers.

"Anklicken, drucken, ausschneiden, sparen", hieß es auf der zugehörigen Webseite. Sie war so präpariert, dass sich schon nach dem ersten Mausklick Wurm Waledac installieren wollte. Waledac hat die Aufgabe, den infizierten Rechner auszuspionieren und sämtliche Passworte mitzuschneiden. Er kann weitere Schadprogramme nachladen und den verseuchten Computer in einen fernsteuerbaren Zombie-PC verwandeln, der dann für cyberkriminelle Zwecke missbraucht wird.

Nutzerstandort per Geolocation

Schon bei der Coupon-Kampagne setzten die Waledac-Verbreiter eine Technik ein, die den Standort des jeweiligen Webseitenbesuchers automatisch in den Text der Webseite einfügte. So konnten vermeintliche Rabatt-Coupons speziell etwa für München, Hamburg oder Dresden angeboten werden - je nach Standort des Webseitenbesuchers. Mit der neuerlichen Spamkampagne wurde diese Geolocation-Technik weiter verfeinert.

Die Schadprogrammverbreiter, die vermutlich aus Russland stammen, nutzen die IP-Adresse, um den Standort des Surfers, der auf die manipulierte Webseite gelockt wurde, ausfindig zu machen. Die IP-Adresse wird automatisch ausgelesen und der zugehörige Ort in einer öffentlich zugänglichen Datenbank nachgeschlagen. Anschließend wird der ermittelte Ortsname so geschickt in den Nachrichtentext eingeflochten, dass der Eindruck entsteht, der behauptete Terroranschlag habe in der Nähe stattgefunden.

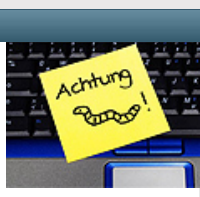
Schutzprogramme werden ausgetrickst

Damit nicht genug. Die Schadprogrammverbreiter ändern ständig den Namen der Datei, die den Schädling installieren soll. Gleichzeitig werden "Aussehen" und Größe dieser Datei immer wieder minimal verändert. Antivirenprogramme sollen dadurch getäuscht werden - mit Erfolg. Das zeigt ein Test, den heute.de über den unabhängigen Analysedienst VirusTotal durchgeführt hat. Das Schadprogramm wurde 39 gängigen Antivirenprogrammen zur Überprüfung präsentiert. Die meisten mussten passen. Nur acht von ihnen erkannten einen Schädling.

Drucken Versenden

zum Seitenanfang

Mehr zum Thema



Conficker: Der Schläfer im PC
Sicherheitsexperten warnen vor neuer Schadprogrammvariante

Liebesgrüße aus dem Virenland
Spammer missbrauchen Valentinstag als Köder

Wurm greift Millionen Computer an
IT-Experten: Schädling schwierig zu entfernen

Angeblicher Obama-Amtsverzicht soll E-Mail-Nutzer leimen
Cyberkriminelle starten Schadprogrammkampagne zur Obama-Amtseinführung

Tauschbörsen: Schädlinge statt Fernsehserien
Bundesamt warnt: Manipulierte Videodateien verbreiten Schadprogramme

2009 gibt es deutlich mehr Cyberkriminalität
Sicherheitsunternehmen mit düsteren Prognosen

Viren-Alarm im Bilderrahmen
Software für digitale Rahmen mit Schadprogramm verseucht

Schnelle Mausklicks mit fatalen Folgen
Gefährliche Fehlalarme bei Antiviren-Scannern verunsichern Nutzer

Externe Links
- Warnung vor Computerwurm Waledac
- Ergebnis der Virenprüfung durch VirusTotal

Das ZDF ist für den Inhalt externer Webseiten nicht verantwortlich

Suche in ZDF.de

Das Unternehmen | ZDFwerbung | ZDFshop | Zuschauerservice | Barrierefreiheit | About ZDF

ZDFinfokanal ZDFdokukanal ZDFtheaterkanal arte 3sat PHOENIX KiKA Deutschlandfunk Deutschlandradio Kultur