COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/conficker-macht-sich-ans-geld-verdienen,1892762

Dornröschenschlaf beendet

Conficker macht sich ans Geld verdienen

Datum: 14.04.2009
Autor(en): Uli Ries

Das Warten hat ein Ende, Conficker zeigt zumindest teilweise, was in ihm steckt: Auf infizierten PCs taucht die Scareware Spyware Protect 2009 auf. Das Ziel der vermeintlichen Schutzsoftware: Unbedarfte Anwender ausnehmen. IT-Sicherheitsexperten haben außerdem entdeckt, dass sich Conficker Anfang Mai teilweise selbst zerstört. Zu schön, um wahr zu sein?

Zeit der Auferstehung: Conficker begann kurz vor Ostern, schädliche Aktivitäten zu zeigen.
Foto:

Kurz vor den Osterfeiertagen beobachteten **Antiviren-Experten**[1], dass mit **Conficker**[2] infizierte PCs die bekannte Scareware Spyware Protect 2009 herunterladen und ausführen. Die Software meldet per lästigem Pop-Up reichlich vermeintliche Infektionen – verrät dabei aber natürlich nichts über Conficker – und verspricht gegen Zahlung von 50 US-Dollar Abhilfe. Microsofts vor wenigen Tagen erschienener **Security Intelligence Report**[3] (SIR) stuft Scareware wie Spyware Protect 2009 als große Gefahr ein. Dies ist die erste wirklich schädliche Aktion, die Conficker seit seinem ersten Auftauchen Ende Oktober 2008 zeigt.

Diese neue, Scareware verbreitende Conficker-Variante wird von Antiviren-Herstellern Conficker.E, Net-Worm.Win32.Kido.js oder auch WORM_DOWNAD.E genannt und sollte inzwischen von allen gängigen Virenscannern entdeckt und entfernt werden. Das perfide an Conficker.E ist, dass er nicht per HTTP herunter geladen, sondern über einen verschlüsselten Peer-2-Peer-Mechanismus zwischen infizierten PCs verteilt wurde. Während alle Welt – allen voran die **Conficker Working Group**[4] – gebannt auf Aktivitäten der von Conficker per kürzlich aufgebohrtem Algorithmus erzeugten Domains wartete, verteilten die Wurm-Entwickler ihre jüngste Schöpfung über eine ebenfalls in Conficker wohnende P2P-Technik und flogen die neue Version somit unter dem Radar ein.

Neben dem Scareware-Download bringt Conficker.E auch eine andere Neuerung mit: Er greift auf eine Domain zu, die seit längerem als Quelle für Infektionen mit dem **Waledac-Wurm**[5] bekannt ist. Das von Conficker.E von dieser Domain heruntergeladene File wurde vor den Osterfeiertagen von **keiner Antiviren-Software**[6] als schädlich erkannt. Aufgrund dieser Verbindung spekulieren Sicherheitsexperten darüber, ob die Autoren von Waledac und Conficker identisch sind.
Rätselhaft ist auch der **Hinweis**[7] in Conficker.E, dass der Wurm sein EXE-File am 03.Mai selbstständig löschen wird. Nachdem die zur Außenkommunikation notwendige DLL jedoch unangetastet bleibt, ist es für Jubelmeldungen über einen digitalen Massenselbstmord zu früh.

Wer wissen möchte, ob sein von Conficker infiziert wurde, sollte sich diese **Testseite**[8] anschauen. Nur wenn alle Logos zu erkennen sind, ist der PC clean. Verwalter größerer Netzwerke sollten eher zu **automatischen Scannern**[9] greifen.

Links im Artikel:

[1] **http://blog.trendmicro.com/downadconficker-watch-new-variant-in-the-mix/**
[2] **http://de.wikipedia.org/wiki/Conficker**
[3] **https://www.computerwoche.de/knowledge_center/security/1892487/**
[4] **http://www.confickerworkinggroup.org/**
[5] **http://www.f-secure.com/v-descs/email-worm_w32_waledac_a.shtml**
[6] **http://garwarner.blogspot.com/2009/04/is-there-conficker-e-waledac-makes-move.html**
[7] **http://www.microsoft.com/security/portal/Entry.aspx?name=Worm:Win32/Conficker.E**
[8] **http://www.confickerworkinggroup.org/infection_test/cfeyechart.html**
[9] **https://www.computerwoche.de/subnet/hp-intel/1891706/**
