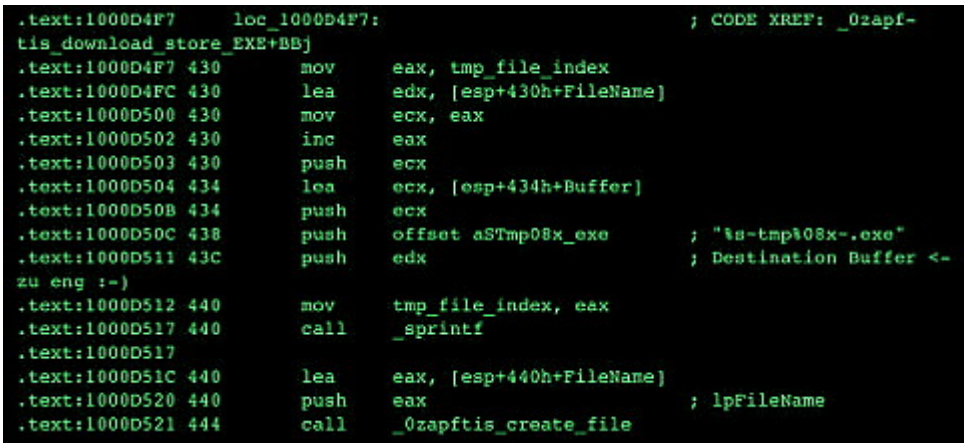
Der Kaiser ist nackt!



Heise meldet, dass die Bundesregierung behaupte, die Software zur Online-Durchsuchung sei einsatzbereit. Das ist aber nicht neu. Wie man der von mir erstellten Chronik der Medienberichte über die so genannte „Online"-Durchsuchung sehen kann, soll das schon vor acht Jahren möglich gewesen sein. Der *Tagesspiegel* titelte am 08.12.2006: „Die Ermittler surfen [sic!!] mit":

"Das System der sogenannten „Online-Durchsuchung" sei bereits in diesem Jahr mehrfach angewandt worden und sei Teil des 132 Millionen Euro schweren Sonderprogramms zur Stärkung der inneren Sicherheit. Die Ermittler sollen sich dabei auf richterliche Anordnung unbemerkt via Internet in die Computer von Privatpersonen einloggen können, gegen die ein Strafverfahren läuft.

(Viele Links funktionieren nicht mehr, aber anhand des genauen Titels kann man sie noch finden, teilweise über archive.org)

Manchmal fühle ich mich wie allein gelassen unter lauter Irren. Was nützt mir ein derartiger Bericht wie der aktuelle bei Heise, wenn niemand fragt, wie die Überwachungssoftware auf den Rechner des „Zielobjekts" gekommen ist? Das ist doch – jenseits der empörten Attitude – eine der wichtigsten Fragen überhaupt? Es braucht doch mindestens den physischen Zugriff (und dann müssen bestimmte Voraussetzungen gegeben sein), oder

das „Opfer“ muss Malware wie Skype schon installiert haben.

Es geht aber mitnichten so, dass jemand „von fern“ irgendwas installiert. Außerdem müsste man ja auch die IP-Adresse wissen und eventuell noch den Router austricksen. (Jetzt fange hier niemand davon an, etwas von „Mail-Attachments“ zu faseln oder von „Websites, auf die man „gelockt“ werden soll. Ich kann es nicht mehr hören.) Christian Rath schrieb in der *taz* am 11.12.2006:

Denkbar sind verschiedene Wege. So kann die Polizei versuchen, ein „Trojanisches Pferd“ (kurz Trojaner) auf den Computer des Betroffenen zu schleusen. Ein Trojaner ist ein Programm, das heimlich Aktionen auf dem Computer ausführt, ohne dass der Benutzer dies bemerkt. Der Trojaner kann zum Beispiel als Anhang mit einer getarnten E-Mail auf den Rechner gelangen. Vorsichtige Computernutzer öffnen aber keine unbekannten Anhänge oder schützen ihren Computer mittels Firewall oder Filter schon vor dem Zugang solcher Spionagesoftware.

Soll ich das jetzt noch kommentieren?

Am 08.10.2011 berichtete Heise:
Dem Chaos Computer Club (CCC) ist nach eigenen Angaben die staatliche Spionagesoftware zugespielt worden, die allgemein unter dem Begriff „Bundestrojaner“ oder in bundeslandspezifischen Versionen beispielsweise auch als „Bayerntrojaner“ bekannt wurde.

In der Analyse des CCC (LESEN!) heisst es: „Die Malware bestand aus einer Windows-DLL ohne exportierte Routinen.“ Ach so. Dann gibt es den „Trojaner“ nicht für Linux? Das ist aber schade.

Wir haben keine Erkenntnisse über das Verfahren, wie die Schadsoftware auf dem Zielrechner installiert wurde. Eine naheliegende Vermutung ist, daß die Angreifer dafür physischen Zugriff auf den Rechner hatten. Andere mögliche Verfahren wären ähnliche Angriffe, wie sie von anderer Malware benutzt

werden, also E-Mail-Attachments oder Drive-By-Downloads von Webseiten. Es gibt auch kommerzielle Anbieter von sogenannten Infection Proxies, die genau diese Installation für Behörden vornehmen

E-Mail-Attachments oder Drive-By-Downloads von Webseiten. Und so etwas schreibt der Chaos Computer Club?! OMG.

Ceterum censeo: Der Kaiser ist nackt!