24C3 | Gezielte Trojaner-Attacken

Laut Heise hat Maarten Van Horenbeeck eine schöne Geschichte über Chinesen-Trojaner erzählt. Ich glaube das alles nicht so einfach. Natürlich: Wenn man „The Month of Kernel Bugs „(MoKB) archive“ anschaut, überkommt einen das Gruseln. Dennoch: Ich halte die meisten Meldungen, die Chinesen hätten wieder irgendetwas „gehackt“, für reine Propaganda, weil niemand die Faken überprüft. (vgl. spiggel.de, 04.09.2007: „Chinesen greifen das Pentagon an!“ sowie spiggel.de, 26.08.2007: „Die China-Hacker kommen nicht“).

„Laut Van Horenbeeck startete die immer wieder mit China in Verbindung gebrachte Trojaner-Invasion 2005 mit einem unauffällig per E-Mail dahergekommenen Bildschirmschoner-Objekt mit dem Namen dot.scr, das eine ausführbare Datei erhielt.“ So ein Quatsch: Warum soll ein Attachment „unauffällig“ sein? Und wer installiert Bildschirmschoner von unbekannten Absendern, womöglich aus China? „2006 folgte gemäß

Van Horenbeeck ein nach wie vor aktiver Trojanerangriff mit einer als HuJintao.doc betitelten Word-Datei.“

Ein Hacker-Angriff mit einer Word-Datei? Womöglich mit einem Bambus-Rechner? Soll ich diesen Schwachfug glauben?

Laut Horenbeck sei die Windows-Schwachstelle MS05-035 ausgenutzt worden. Nach Heise befasst sich MS05-035 „… mit einem Fehler in der Font-Behandlung von Word, der sich durch manipulierte DOC-Dateien ausnutzen lässt. Betroffen ist Word aus Office 2000 und XP (2002) sowie die Word-Versionen aus Microsoft Works 2000 bis 2004. Word 2003 hingegen ist laut Microsoft immun.“ Sehr gefährlich hört sich das nicht an, denn es betrifft nur einige Systeme – und die müsste jemand vorher kennen.

„Im April erregte ein ungewöhnlicherweise in einem reinen HTML-Anhang daherkommender Trojaner die Aufmerksamkeit des Belgiers.“ Mir scheint dieser Belgier ein Wichtigtuer zu sein, mit Verlaub. Anhang in HTML! Da lachen ja die Hühner! Wie

sollte man jemanden, der mit seinem MUA vernünftig umgehen kann, damit überlisten können – und dann vielleicht auch noch *ohne* Javascript? Nein, nein, nein, ich glaube weiterhin kein Wort.

Eine wichtige Quelle für die angeblichen Trojaner-Angriffe aus China ist jemand, der keinen Anlass auslässt, um sich zu blamieren: „Die Beamten im Innenministerium haben die angeblich aus China stammenden Trojaner-Angriffe auf Bundesbehörden nachdenklich gemacht. ‚Finstere dritte Mächte' hätten entsprechende Versuche unternommen, weiß Staatssekretär August Hanning. Diese seien aber „erfolgreich abgewehrt worden". (Heise-Newsticker, 05.09.2007)

Vielleicht wäre es an der Zeit, wenn der geschätzte Kollege Krempl, der fast alle die Meldungen bei Heise verfasst hat, die Zeit fände, auch einmal die Fakten zu überprüfen – dann löste sich der Trojaner-Hoax made in VR China vermutlich in Luft oder in Praktikanten auf.