Computervirus befällt Word-Dokumente

Computerviren infizieren nur ausführbare Programme? Irrtum! Eine neue Generation dieser digitalen Schädlinge befällt und verbreitet sich über Word-Dokument-Dateien. Es reicht das Öffnen und Lesen eines infizierten Dokumentes um andere Dokumente und auch den Computer zu infizieren.

Dieter Göschler

Ende August '95 wurde das erste Mal das Auftreten eines Virus festgestellt, der Microsoft Word Dokumente und Dokumentvorlagen infiziert und damit als Basis seiner virulenten Tätigkeiten benutzt. Der Virus ist unter dem Namen *WordMacro.Concept* bekannt, auch die Namen *WinWord.Concept, WW6, WW6Macro und PrankMacro* werden verwendet. Dieser erste Makro-Virus hat noch keine destruktive Schadenfunktion, und die Erkennung und Entfernung des Virus ist verhältnismäßig einfach, er stellt aber durch sein simples Konzept die Basis für eine mögliche Flut von möglicherweise aggressiveren Nachbildungen dar. Das Wissen um die Gefahr beim Öffnen fremder, unbekannter Dokumente kann Schaden verhindern.

Die Möglichkeiten der Verbreitung über Dokument-Dateien ist nicht überraschend, die Gemeinschaft der weltweiten Virenexperten kennt bereits seit mehreren Jahren die Möglichkeit, mit Hilfe von Makroviren aktive Dokumente zu befallen und Computer zu manipulieren.

Wie funktionieren diese neuen Viren?

Wenn mit MS-Word ein Dokument erstellt wird, so werden in dieser Dokumentendatei neben dem eigentlichen Text auch noch andere Dinge wie etwa Grafiken, Schriften oder auch Makros mitgespeichert.

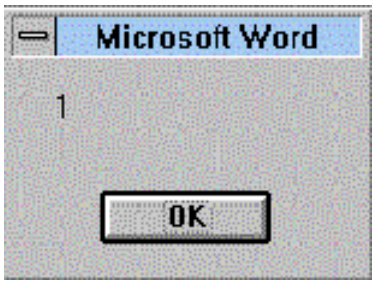
Auf diese Eigenschaft von MS-Word und seiner Dokumente baut nun der Virus auf. Der Virus ist in der Makrosprache von Microsoft Word geschrieben, in Word BASIC, ein proprietärer Dialekt der schon recht betagten Programmiersprache BASIC. Er befällt Dokumente und Dokumentenvorlagen (normalerweise mit den Namenserweiterungen `DOC` und `DOT`). Der Virus ist funktionsfähig unter Microsoft Word für Windows 6.0, auch über die Version Word für Macintosh verbreitet sich der Virus. Damit ist dieser Virus multiplattformfähig und teilweise betriebssystemunabhängig.

Der Virus besteht aus einer Reihe von Word Makros, welche im Dokument mitgespeichert sind. Mit der Ausführung dieser Makros pflanzt sich der Virus fort. „Nun gut", werden Sie sagen, „wenn ich diese Makros nicht starte, kann sich auch der Virus nicht verbreiten". Dies stimmt, allerdings nur teilweise.

Der Befall kann nicht verhindert werden!

Wenn mit MS-Word ein Dokument geöffnet wird, kontrolliert die Textverarbeitung als erstes, ob in diesem Dokument nicht ein bestimmtes Makro vorhanden ist (Name aus Sicherheitsgründen gestrichen). Existiert dieses Makro, wird es automatisch ausgeführt. Damit wird der Virus aktiv, ohne daß es der Benutzer verhindern kann oder ein Makro selbst starten zu müssen.

In infizierten Dokumenten existiert dieses Makro zusammen mit einigen anderen. Wird es nun zum Lesen geöffnet, startet automatisch dieses Makro und überprüft, ob die restlichen Viren-Makros bereits im globalen Makro-Pool bzw. in der globalen Dokumentenvorlage `NORMAL.DOT` vorhanden sind. Falls nicht, wird diese infiziert. und ein kleines Popup-Fenster am Bildschirm als Zeichen der erfolgreichen Manipulation angezeigt. Dieses Fenster trägt die Überschrift „Microsoft WORD" und enthält nichts außer einer einzelnen Zahl (für gewöhnlich eine „1").



An diesem einmaligen Aufpoppen eines unüblichen Fensters kann eine Verseuchung erkannt werden.

Ab diesem Zeitpunkt wird jedes weitere Dokument infiziert. Jedesmal, wenn ein neues Dokument geöffnet/erstellt wird, kopieren sich die Viren-Makros in das Dokument, wenn dieses Dokument mit Hilfe der „Save As" Funktion abgespeichert wird. Beim Aufruf dieser Funktion infiziert der Virus das Dokument dadurch, daß seine eigenen Makros in das zu sichernde Dokument kopiert werden (auch das automatisch geöffnete Makro). Wenn ein infiziertes Dokument später auf einem anderen Rechner geöffnet wird, wird dort die Datei NORMAL.DOT infiziert und der Virus breitet sich weiter aus.

Wie kann ich diesen Virus erkennen?

Am einfachsten und sichersten schützen Sie sich mit bewährten Virenschutzprogrammen. Berücksichtigen Sie aber bitte, daß das Virenschutzprogramm grundsätzlich nicht `*.DOC`- oder `*.DOT`- Dateien untersucht. Dies müssen Sie in den zu überprüfenden Dateierweiterungen (Default-Extentions) einstellen.

Haben Sie kein gutes Anti-Viren-Tool zur Hand, gibt es auch die Möglichkeit, den Virus "manuell" aufzuspüren.

Wenn auf einem sauberen System mit nicht infizierter `NORMAL.DOT` Datei das erste Mal ein befallenes Dokument geöffnet wird, wird eine kleine Popup Box am Schirm angezeigt. Diese trägt den Titel „Microsoft Word" und enthält eine einzelne Nummer, normalerweise eine Eins ('1'). In Word für Macintosh erscheinen befallene Dokumente mit dem Druckvorlage-Icon anstatt mit dem Dokument-Icon, daß normalerweise verwendet wird. Danach wird die Word-Konfigurationsdatei `WINWORD6.INI` manipuliert und der Eintrag `WW6I=1` hineinkopiert.

An diesen beiden Veränderungen können Sie erkennen, ob Ihr Computer bereits befallen ist.

Desweiteren verändert der Virus die Makro-Liste. Finden Sie also in Ihrer Makro-Liste Ihnen unbekannte oder eigenartig klingende Makros wie `AAAZA0` oder `PayLoad`, so könnte es sich um einen Teil eines Makro-Virus handeln.

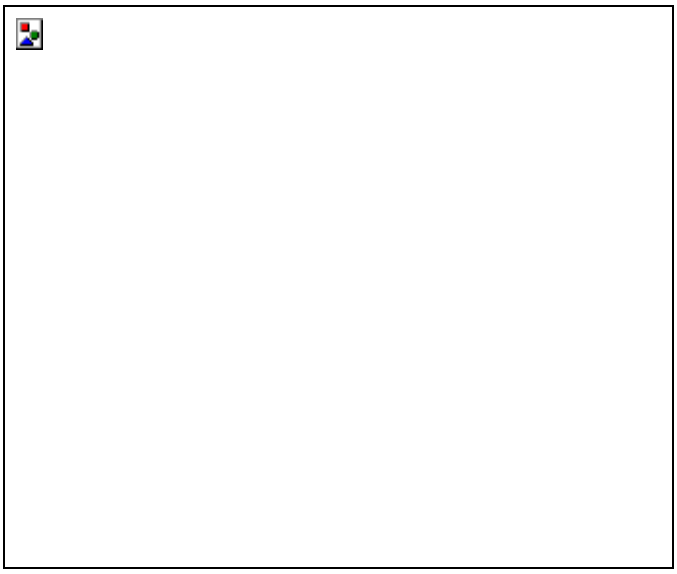


Abbildung der Makro-Liste einer befallenen Maschine

Kann ich diesen Virus wieder entfernen?

Um den Virus manuell zu entfernen, sind folgende Schritte notwendig:

- das befallene Dokument öffnen
- im Hauptmenü Punkt „Extras“ auswählen
- den Menüpunkt „Makro“ auswählen
- die Makros aus dem Dokument entfernen
- das Dokument mittels Punkt „*Speichern*“ unter Menüpunkt „*Datei*“ abspeichern (NICHT mittels „*Speichern unter...*“ !!)

Sobald alle anderen Dokumente desinfiziert sind, öffnet man die Dokumentenvorlage `NORMAL.DOT` (üblicherweise im `\WINWORD\TEMPLATE` oder Vorlagen-Verzeichnis), und führt die oben genannten Schritte zum Entfernen der Makros durch. Nach dem Speichern der `Datei NORMAL.DOT` mittels „*Speichern*“ sollte man Word beenden.

Vergessen Sie aber bitte nicht, auch infizierte Dokumente, die nicht benötigt werden, sollten gelöscht werden.

Falls in einigen Dokumenten Makros vorhanden sind, die noch benötigt werden, kann man auch nur die Viren Makros entfernen. Ihre Namen sind `AutoOpen`, `FileSaveAs`, `PayLoad`, `AAAZAO` und `AAAZFS`. Das „`PayLoad`“ Makro enthält interessanterweise nur folgenden Text:

```
Sub MAIN
       REM That's enough to prove my point
End Sub
```

Dieses Makro wird aber nie aufgerufen. Durch die Flexibilität der Makrosprache von Microsoft's Word BASIC könnte aber hier nahezu jede vorstellbare Schadensfunktion implementiert werden.

Daß diese Möglichkeiten von Virenprogrammierern auch genutzt werden, zeigt ein weiteres aggressiveres Beispiel eines Makro-Virus, doch davon später.

Zu beachten ist, daß das Vorhandensein eines Makros namens `AutoOpen` oder `FileSaveAs` in einem Dokument nicht unbedingt auf die Präsenz des Virus hindeutet. Diese Namen werden auch von völlig legitimen nicht viralen Makros verwendet.

Weiters sollte beachtet werden. daß Word in vielen verschiedenen Sprachen erhältlich ist, und in manchen Versionen sind auch die Kommandos der Makrosprache in die jeweilige Landessprache übersetzt worden. Das hat den Effekt das zum Beispiel Makros die mit der englischen Version geschrieben wurden, nicht in der finnischen Version verwendet werden können. Dadurch werden Benutzer solch einer nationalen Version nicht vom Virus infiziert. Die Verwendung eines befallenen Dokuments in einer übersetzten Version von Word verursacht aber keinerlei Fehlermeldung, und die Infektion bleibt auch bei einem neuerlichen Abspeichern des Dokuments funktionsfähig. Diese Gruppe von Anwendern sollte instruiert werden, Dokumente immer auf die Präsenz des Virus zu untersuchen, um eine Weiterverbreitung infizierter DOC-Dateien zu vermeiden.

Vorsorge

Der zuverlässigste Weg um eine Infektion zu verhindern ist die Überprüfung sämtlicher eingehender Word Dokumente auf die Präsenz des Virus. Es gibt auch verschiedene Möglichkeiten, den Virus an der Infektion des Systems zu hindern, wenn ein infiziertes Dokument irrtümlich geöffnet wird.

Dieser spezielle Virus wird die Datei `NORMAL.DOT` nicht befallen, wenn er ein bereits vorhandenes Makro namens „`PayLoad`“ findet. Diese Vorsorge hindert aber andere gleich aufgebaute aber im Detail unterschiedliche Viren nicht an der Infektion des Systems. Verschiedene Funktionen von Word können verwendet werden, um die „`Auto`“ Makros abzuschalten, die dieser Virus und andere gleichartige Viren benutzen, um sich zu verbreiten. Manche benötigte Funktionen von Word Dokumenten können aber auf diese „`Auto`“ Makros angewiesen sein, und das Abschalten dieser Makros könnte diese Funktionen unverwendbar machen. Außerdem könnte das „`AutoOpen`“ Makro mit geringem Aufwand so modifiziert werden, daß die Dokumentenvorlage unabhängig von der Existenz eines „`PayLoad`“ oder „FileSaveAs“ Makros befallen wird.

Schreibschutz der `NORMAL.DOT`:

Eine andere Präventivmaßnahme ist das Aktivieren der Abfrage „*Automatische Anfrage für Speicherung von NORMAL.DOT*“. Diese Menüpunkt ist erreichbar auf der „*Speichern*“-Seite des Punktes „*Optionen*“ unter dem Menüpunkt „*Extras*“. Wenn diese Option aktiviert ist und irgendein Prozeß (auch ein Virus Makro) eine Änderung der Inhalte des normalen globalen Datenpools verursacht, wird der Anwender vor dem Speichern dieser Änderungen auf der Platte um Zustimmung gefragt. Unglücklicherweise enthält der Wortlaut dieser Anfrage keinen Hinweis, daß diese Änderungen schädliche Auswirkungen haben können. Daher ist es wichtig, die Benutzer soweit zu schulen, daß sie nicht automatisch „Ja“ auf diese Anfrage antworten, falls man diese Option als Präventive verwenden möchte.

Was kommt danach?

Die neu entdeckten Möglichkeiten der Virenprogrammierung in Makrosprachen macht es verwirrten Gehirnen wieder einfacher, Viren zu schreiben.

Der WinWord.Nuclear-Virus, ein weiterer neuer Makro-Virus besteht eigentlich aus zwei Viren. Der erste Teil des Virus fügt bei jedem Dokument vor einem Ausdruck einen Text an, so daß jedes Dokument mit dem Zitat

> “And finaly I would like to say: STOP ALL FRENCH NUCLEAR TESTING IN THE PAZIFIC”!

endet. Dies ist besonders ärgerlich beim automatischen Versenden von Fax-Dokumenten. Der zweite wesentlich aggressivere Teil des Virus löst sich mit einigen Tricks aus der Makrosprachenwelt und installiert sich unbemerkt wie ein klassischer Virus in COM/EXE-Programmen. Während der erste Teil “nur” störend wirkt, **löscht der zweite jeden 5. April die Systemdateien des Betriebssystems**.

Conclusio

Makroviren nutzen keine neuen Möglichkeiten und sind relativ einfach bekämpfbar. Die Einfachheit der Programmierung wird möglicherweise der Vermehrung stark beitragen. Mit dem Wissen um die Gefahr und ein wenig Umsicht werden sich Makroviren jedoch nicht weit ausbreiten können. □