



## **Macro Rebound: The “New” Trojan Dropper?**

**infectionvectors.com**

**August 2004**

### **Overview**

Macro viruses represent a proven method of compromising hosts. Further, they execute within a trusted application, often one used to construct private documents. Since their first appearance nearly 10 years ago, macro viruses have remained rather benign. There are those that attempt delete system files, however, as a family, the macro viruses don't produce a great deal of fear in security administrators. Many companies that follow the “defense in depth” practice allow email attachments with “.doc” or .xls” through the mail relays with no hesitation. They are more than willing to rely upon a single layer, the host antivirus software to stop the macro. The trend in blended threat viruses may be signaling a move to use macros as transmission mechanism (or a dropper) for malicious payload, however. The report below outlines the beginnings of macro viruses, and where they may be heading.

### **The Macro Virus**

The use of VBA and the MS Office suite as a medium for viruses is by no means a new concept. Macro worms have been part of an MS Word user's world since the mid 1990's. One of the first widespread macro viruses was Concept (Prank). Macros represented a new means of compromising machines, by asking a user to simply read a document in a trusted file format. There were no obscure file extensions and they often had familiar names. The spring of 1999 saw what is still the most famous macro, Melissa (in fact, a Google search of macro+virus yields numerous hits for Melissa). Although Melissa did email potentially proprietary or secret data out of an organization, it did not deliver the types of payloads security professionals would currently expect (such as a backdoor routine of some type, author notifications, file destruction, etc.). Melissa arrived via email, and then infected MS Word documents, sending a copy of an infected document to 50 people via MS Outlook. New macros viruses are written and distributed everyday.

New macros viruses do not receive the attention they once did as security features built into MS Office products have gone a long way to preventing widespread outbreaks that occurred prior to Office 2000. In addition, most of the macro viruses of late have not carried a payload that was particularly scary. They are slow spreading worms, mostly in the category of “nuisance” with most security administrators.

## Propagation

The success of a macro virus lies in the trust most people have for “.doc” files. Further, the extended reach of the MS Office suite allows for a wide selection of propagation mechanisms. At its heart, the macro can infect the template “Normal.dot,” so that future documents receive a copy of the macro. The hooks within MS Word could allow for download and execution of code, connection to IRC channels, and disabling security software. In fact, each of these has been successfully implemented into a macro. These actions sounds remarkably similar to those carried out by some of the most damaging mass mailers and Internet worms.

## Macro-biotics

Macros have had a somewhat innocuous lifespan in terms of the magnitude of their impact. Recently, however, new uses for MS Word macros have been developed and released. These macros attempt to do the same things as viruses such as Agobot, Netsky, and Kibuv (among many others). A brief outline of a few macros found since last year:

<u>Macro Name</u>	<u>Primary Function</u>
W97M.MLHRDrops	Trojan/Changes homepage
W97M.Nobody	Deletes AV Signatures\Create IRC Script
W97M.Asmah	Mass Mail
W97M.Smey	Trojan Dropper (Corrupts MBR)
W97M.Evo	Disables Word Macro Protection/Destructive/mIRC
W97M.Adren	Template Infection/Registry Modifications
W97M.Ortant	Deletes AV software
W97M.Tabi.Trojan	Downloads/executes file
W97M.Kingpaw.A	Adapts to IRC client of Host
W97M.X3	Drops Trojan

Quick analysis of these macros (many of which could be given the name “Trojan,” “Worm,” or “Virus”) shows that it is possible that tomorrow’s mass mailer could easily utilize “report.doc” as an attachment that would, upon opening, download and execute additional viral code.

Another possibility is that the macro will be the payload itself of other, proven methods of distributing viruses. Instead of the “.doc” being the primary mechanism to infect a machine, it could be used as the distribution engine only. Consider how some viruses come preloaded with a list of antivirus clients to disable (such as the lengthy list in Agobot) or make Registry changes (almost every new Windows virus). If one of these changes were to disable macro security in Office, then infecting the “Normal.dot” file would not trigger an alert when MS Word is fired up (along the lines of adjusting the settings in HKEY\_CURRENT\_USER\Software\Microsoft\Office\9.0\Word\Security). In either case, the power of macros will likely be tapped again with at least moderate success.

The appearance of these new functions after a period of relative stagnation in macro innovation may be a coincidence. However, it may be signaling a movement of virus writers into a “new” area of kicking off viral attacks. Periodically revising infection vectors gives a virus writer options when selecting one or more means of delivering a piece of malicious code. Recent trends have shown that multiple vectors will be glued together within a single virus, increasing the chances of a successful infection. This experimentation with macros may be another mechanism for keeping things fresh.

### **Blocking Macro Attacks**

Macros, of course, have to be enabled to run. By default, Word 2000 sets macro security to “High,” meaning that unsigned macros are silently disabled. Crafting a falsified digital signature for a macro is no trivial task, making it an unlikely, but far from impossible possibility. Those users at a high risk for infection are those that have changed the macro security settings to Medium or Low. These would allow a macro to run automatically or after the user clicks “OK,” to a warning from MS Word. This warning is similar to those presented by Outlook for opening attachments that are executables, which has proven to be ignored by many users. Furthermore, older copies of MS Office, such as Office 97, do not have the same levels of security for blocking macros (keep in mind the rampant success of Melissa).

Moreover, most antivirus software is quite adept at identifying malicious macro code. Of course, if everyone had antivirus software running properly, there would be a much smaller market for viruses than there is today.

Is it possible that the day is not far off when “.doc” is blocked as readily as “.exe”? The initial success of worms that employ macros to propagate will be important. If widespread infections are the result of one of these macros, other virus writers may take notice and invest time into improving the medium.

The threat from macro viruses still remains low, however, in response to the numerous new efforts to improve the viral properties of macros, it is a good time to ensure that MS Office macro settings are in line with the security posture of your organization.

## References

General Macro History:

Description of the Concept macro: <http://www.f-secure.com/v-descs/concept.shtml>

Kaspersky's Macro History: <http://www.viruslist.com/eng/viruslistbooks.html?id=15>

F-Secure Melissa & variants report: <http://www.f-secure.com/v-descs/melissa.shtml>

Melissa CERT advisory <http://www.cert.org/advisories/CA-1999-04.html>

Macros Mentioned in "Macro-biotics" section:

Tabi: <http://securityresponse.symantec.com/avcenter/venc/data/w97m.tabi.trojan.html>

Nobody: <http://securityresponse.symantec.com/avcenter/venc/data/w97m.nobody.html>

Smey: [http://secunia.com/virus\\_information/9037/w97m.smey/](http://secunia.com/virus_information/9037/w97m.smey/)

Ortant: <http://www.sophos.com/virusinfo/analyses/wm97ortanta.html>

X3: [http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ\\_X3.A](http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_X3.A)

Kingpaw: <http://www.sophos.com/virusinfo/analyses/wm97kingpawna.html>

Evo: <http://www.symantec.com/avcenter/venc/data/w97m.evo.html>

Adren: <http://securityresponse.symantec.com/avcenter/venc/data/w97m.adren.html>

Asmah: <http://securityresponse.symantec.com/avcenter/venc/data/w97m.asmah.a.html>

MLHR: <http://www.symantec.com/avcenter/venc/data/w97m.mlhr.html>

Office Security Links:

Microsoft's Word 2000 default security settings (mentions Melissa as example):

<http://support.microsoft.com/default.aspx?kbid=224506>

Office 2000 Macro Security:

<http://www.microsoft.com/technet/prodtechnol/office/office2000/maintain/security/o2ksec.mspc>

Copyright © 2004 infectionvectors.com. All rights reserved.