FEATURE SERIES 2

Lotus Notes and Email Risks – Part 1

Martin Overton
ChekWARE, UK

The re-emergence of Worms earlier this year, coupled with the current tendency of virus writers to make their progeny 'Internet-aware' and with the growing trend of companies rationalising their software systems (known as standardising) means that the risk from viruses targeted at a particular infrastructure has increased dramatically. Many big corporations and smaller companies are standardising on *Lotus Notes* as their Groupware solution. It is estimated that there are 35,000,000 licensed *Notes* users worldwide (October 1999). Let's have a look at the strengths and weaknesses of this approach, specifically the email features.

Let me make one thing very, very clear. *Lotus Notes* has always had security built in and is, to the best of my knowledge, the most secure Groupware solution currently on the market. This does not mean, however, that it cannot be attacked; it just means that if it is properly installed and configured that the risks of attack are minimized, or in some cases neutralised.

One thing you must be aware of though is that, by default, *Notes* client installations (straight from the box) have most of the excellent security facilities turned off! I wonder just how many companies are running *Notes* clients in this way?

Let's get down to business. I will start by covering the potential risks (not touching on hoax viruses which, although an email-related problem, are beyond the bounds of this article) of using *Notes* clients in its 'out-of-the-box' state i.e. worst case scenario, and then move onto how these risks can be addressed, removed or where no solution is available, at least understood.

I believe that at the moment email (both attachments and scripting) is the biggest threat to users, and this shows no sign of changing soon. Indeed, the recent appearance of 'BubbleBoy', 'MyPics' and the numerous new Melissa variants indicates that this vector has become the main choice for many virus writers and other malcontents.

What are the Risks?

Well, there are two types of threat here, existing viruses and *Notes*-specific threats.

The risk to *Notes* users from existing viruses (macro, executable, boot, etc), which makes up the largest slice of the *Notes* email risk pie, can generally be summed up in one word; attachments!

Let's look at this in more detail:

Files (EXE, COM, DLL, SYS, SCR, HLP, etc)

The main threats here appear to be (at the time of writing) Worms such as Win32/Ska and Win32/ExploreZip, and a myriad of Trojans such as the ubiquitous *AOL* password-stealers. As this article goes to press, the trend seems to be accelerating, Win95/Babylonia being the latest example. The original file infectors still seem prone to slow propagation, unless they get lucky, and this is borne out by the low figures found in the *Virus Bulletin* Prevalence Table.

Boot Sector Viruses (MBR and DBR)

These are still a problem, although the number of outbreaks is still small, and the risks in an email scenario are minimal. This class of virus can still be sent as an attachment, though this requires a metamorphosis into a 'dropper', 'DEBUG Script', disk image format or other intermediate state.

Macros (*MS Office*, *Word Perfect Office*, etc)

Recently, macro viruses have been seen to account for around 80% of reports in the *VB* Prevalence Table. They present the biggest threat to companies, since *Office* files are passed around with, in too many cases, wild abandon.

This is compounded by the number of people who use *Word* as their default *Notes* email editor. Either that, or they blindly 'launch' attachments in their native *Office* applications. If the viral macros are not intercepted by any AV software, and they are run, the *Office* application environment becomes infected.

Scripts (JavaScript, VBScript, *WSH* files, etc)

VBS/BubbleBoy has shown that the scenario I outlined in my VB'99 paper is valid, although that Worm is targeted at *Outlook*/*Outlook Express* rather than *Notes*. *Notes* can also run code when an email is either pre-viewed or opened and therefore could be used to launch a similar Worm without the use of any attachment.

HTML sent to *Notes* could have VBScript (including *WSH*) or JavaScript embedded in it, which will trigger if opened in a browser that supports it. *Notes* allows you to choose which internal browser to use with *Notes*. *Lotus*/*IBM* offer their own browser, or you can choose to use either *Microsoft Internet Explorer 4.x* (or later) or *Netscape 4.x* instead.

It is certainly possible that a virus such as VBS/BubbleBoy could trigger when an HTML attachment is launched from *Notes* into *Internet Explorer* (always assuming that the remaining requirements are also met for it to trigger either partially or completely).

Extract from 'Viruses and Lotus Notes: Have Virus Writers Finally Met Their Match?'

'*Because of the power of* Notes *macros and other scripting languages, which are either part of* Notes *or are supported by* Notes *this auto-launching can occur!*

What's worse is that infected files using auto-launching can also be despatched to hundreds of users via email before they are detected, at the least this can cause a mail storm, at worst it could cause loss or theft of critical data and even publishing of sensitive data to the internet as in the PolyPoster and Caligula viruses.'

As for the *Notes*-specific threats – let me make it quite clear that, as at the time of writing there are no *Notes*-specific viruses known. Current threats are limited to Trojans, possible Denial of Service attacks and mail bombs. I do believe that viruses and Worms can be created within *Lotus Notes*. Let's look at the risks of each function/threats:

Trojans

In earlier versions of *Notes* (pre-*4.5*) Trojans, unlike mail bombs, required assistance from the user to trigger. This does not make Trojans any less dangerous, or less likely to be activated, as the number of victims of Trojans and Worms can attest to. With *v4.5* or later, this user assistance is now no longer required; simply opening (reading) or previewing a *Notes* email (sent from another *Notes* client) can launch an attachment or run code.

The features employed to create Trojans are everyday *Notes* elements which users handle without a second thought. The main *Notes* features open to such abuse are Buttons and Hotspots (popups and action hotspots). Since the arrival of *Notes v4.5*, the latter are a particular danger because they also allow the use of @Commands. Before that version, popups could only be used to display help text – now you can attach more than just *Notes* formulae to Action Hotspots; this can include LotusScript or JavaScript.

Mail Bombs

There are currently two main types of mail bomb: stored forms and self-launching OLE objects. The former will *force* a document into a stored form by saving (and sending) that stored form with the document. This is particularly effective when used with a 'computed for display' type field in the stored form. This can be used to initiate a predefined string of events, benign or devastating depending on the author's intent. Many mail bombs will go off with (little or) no user intervention. Merely opening one up is sufficient – as simple as viewing or previewing the email.

LotusScript

This is, in many ways, very similar to *Microsoft's* VBA. This, I believe, will soon give rise to LotusScript viruses, Trojans and Worms. LotusScript can include calls to external files, *Notes* APIs and *Notes* functions. This can readily be used to manipulate the user's mail file and any other databases that the user has manager rights to. By default, a user has manager rights to their mail database. It is possible that LotusScript could become the Achilles' heel of *Notes*, as VBA is to *Microsoft Office* applications, and we are all only too aware what that brought forth! It is rumoured that *Lotus* will be ditching LotusScript in the next release of *Notes* and just supporting JavaScript.

Indeed, I have already seen code samples that do run when an email is opened (read) or even previewed in the *Notes* client preview pane.

Stored Forms

Stored forms were first introduced in *Notes v2.0* and have since been considered a security threat by many *Notes* administrators. Stored forms can contain Formulae, JavaScript or LotusScript that can be triggered when the email is opened or even previewed.

OLE

According to *Lotus*, '*Object Linking and Embedding (OLE) is a technology that lets you share data between applications and is supported for Windows and Macintosh. OLE lets you link or embed data from other applications, such as a 1-2-3 chart, Word Pro document, or Freelance Graphics presentation, in a Notes document. You can embed or link part of a file or a whole file. You can also embed a new object in a Notes document and use the object's application to enter data in Notes. For example, if you have 1-2-3, you could create a blank 1-2-3 worksheet object and enter 1-2-3 worksheet data in a Notes document.*'

Formulas and Field Formulas

Lotus defines formulas thus – '*An expression that has program-like attributes; for example, you can assign values to variables and use a limited control logic. Formulas are best used for working within the object that the user is currently processing. The formula language interface to Notes and Domino is through calls to @functions.*

You can write formulas that return a value to a field, determine selection criteria for a view, create specific fields in a form, determine the documents a replica receives, help users fill out a document, increase database performance, and create buttons or hotspots.'

In Summary

There is certainly a possibility that a Melissa-type email Worm/virus can be written to target *Lotus Notes*. All the functionality is there and in its 'out-of-the-box' state *Notes* offers little resistance to these threats. The second part of this article, to be featured in next month's issue, will deal with what can be done to minimize or neutralise the risks outlined above.