FEATURE SERIES 2

Lotus Notes and Email Risks – Part 2

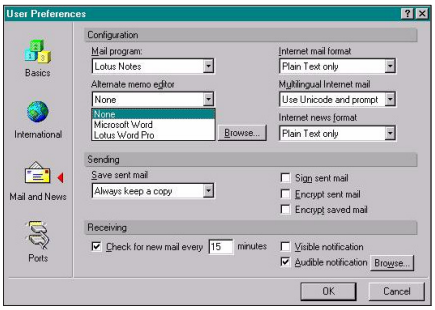
Martin Overton
ChekWARE, UK

Last month I covered most of the email risks posed by malware to *Lotus Notes* in its 'out-of-the-box' state, i.e. the worst case scenario. This second part of the series will address how to use the in-built security features in *Lotus Notes* to neutralise (where possible) or minimize the identified threats.

Addressing the Risks

Lotus Notes offers a few options to help minimize the threat from existing classes of viruses. I will look at these briefly below, and cover the *Notes*-specific functions later.

Let us look at macro viruses first, as they constitute the largest percentage of outbreaks each month. Currently, *Lotus Notes* does not allow you to stop attached OLE compound files which are infected from being launched by a user's intervention (loaded into *Word*, *Excel* etc). What you can do is encourage the use of the View option on the attachment dialog. This will allow you to read the *Microsoft Office* file without running any macros or VBA within the document or spreadsheet. Also, ensure that the default Document Memo Editor is set to None, rather than *Word* or *Lotus WordPro* (see picture below).



Encourage the use of portable document formats that cannot contain VBA code, such as *Adobe Acrobat*. I would have suggested Rich Text Format (RTF) but this can easily be subverted (as illustrated by WM/Cap) and therefore, unless you are prepared to inspect the file format with a hex or ASCII editor, you cannot be 100% sure that the file really is an RTF file. Even if it is, please be aware that while macros are stripped, any embedded objects (which may contain viral content) are not.

Apart from banning executable attachments (like COM and EXE) which, unfortunately, is looking more and more attractive and even good policy, there is little more that you can currently do to reduce the risk of file infectors. Let's put this into perspective though – this risk (until recently) only accounted for around 5% of reported virus outbreaks each month. I do not mean that it is a non-threat, but it does need to be taken in context against the preponderance of macro viruses.

Disk images are not generally passed around but the associated risk, while small, needs to be understood. Prevalence tables indicate that Boot Sector viruses average around 10% of all monthly virus outbreaks. The most prudent solution is to ban disk images in much the same way as executable attachments.

1999 appears to have seen the revival of file-type malware, especially Worms like W32/Ska (aka Happy99) and the many W32/Explore.Zip variants. In fact, the former appears to have caused the reports of file-infecting/affecting malware outbreaks to jump to over 16% in April of 1999 and average out at around 12% for the rest of the year. There seems to be little that *Lotus Notes 4.6/5.0* security features can do about them.

Any Good News?

With *Notes 4.6* or *5.0* there is a security facility known as the ECL (Execution Control List). The ECL – in *Notes 5.0* there are three distinct ECLs – allows you to restrict access to specific functions that code embedded in the *Notes* email (or other *Notes* document/form) can use, if allowed. The ECL is controlled via the use of digital signatures which allow you to restrict/grant access to functions by a specific signature or lack thereof.

This is best thought of as a type of Access Control or Behaviour Blocking. It does *not* mean that the signed code is safe, just that it is signed. All this gives you is proof that the code was signed by its owner and has not been changed since its signing, nothing more.

ECLs *only* affect the email's embedded auto-run (auto-execute) code, which may be used to auto-launch an attachment or any number of other functions. This does *not* stop a user running an attachment or clicking on a button or hotspot, thereby launching a Trojan, Worm, virus or other code behind these functions. When an ECL rule is triggered (i.e. a signature or lack of signature exceeds the bounds of its authorized security settings) an ECL pop-up box will appear (see below) which offers the option to trust the code and the signatory of it.

This, at least, gives you non-repudiation as a stick to beat the signatory with in case of unwanted effects, such as a Worm, virus or other malware. But, and it is a big but, this dialog box still allows the user to accept/run the embedded code/action (trust the signatory, once or always). Haven't we seen this type of approach somewhere before? If in doubt, delegate the responsibility to the user, then it is their mistake!

VIRUS BULLETIN

ECL Setting

Lotus says: '*By default, no scripts or formulas, whether signed or unsigned, can execute on your workstation without displaying a warning message. However, scripts or formulas run from any database created with a template that ships with* Notes *are signed "Lotus Notes Template Development/Lotus Notes", and this signature has complete execution access* [including the mail database template].'

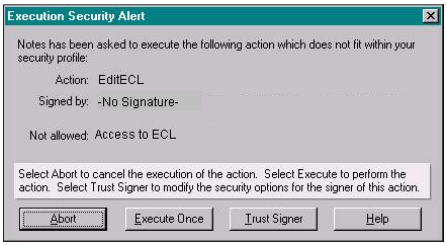
Workstation security limits the following:

- Access to the file system
- Access to the current database
- Access to environment variables
- Access to non-*Notes* databases
- Access to external code
- Access to external programs (this option affects the ability to create or modify OLE objects)
- Ability to send mail
- Ability to read databases other than the current one
- Ability to modify databases other than the current one
- Ability to export data
- Access to the Workstation Security ECL

Using wildcards in the execution control list: *'You can enter a wildcard in a name in the execution control list, thus extending access to everyone whose hierarchical name contains a particular element. For example, you can enter */Acme to extend access to all users whose hierarchical names end in /Acme.'*

As you can see, the key here is that the ECL settings only affect agents, scripts and macro functions included in databases, forms and fields, *not* attachments.

The dialog box below shows what happens when an ECL setting is tripped, in this case, to *Edit ECL* for the workstation. This would allow the workstation (clients) security level to be altered to anything the author intended!



Get the feeling that you could be looking at the macro warning dialog in *Microsoft Word 97* or *Excel 97*? I wonder just how many users would just click 'Trust Signer' without thinking, just as they do for *Office* Macro warnings? This risk can be removed by the Administrator locking the clients' access to change their ECL.

Interestingly, *Lotus* added the further option to ECLs in *Notes 5.0*. You can also restrict access to signed Java applets and JavaScript applications. Select either 'Java applet security' or 'JavaScript security' in the Execution Control List and go through the list of access options you want to give to each signatory.

A user who shares a computer with others can set up his or her own ECL. The ECLs are unique to each person's User ID. Yet *Lotus* still offers no option to restrict the launching or detaching of file attachments by the users themselves. One wonders why not? Surely offering such a facility would ultimately help to negate some of the risks posed by sharing *Office* files?

Of course, I am playing devil's advocate here. No current groupware/*Office* Suite offers anywhere near the level of security that *Notes*/*Domino* offers. Nevertheless, I would like to see this feature added.

Let us take a look at this proposed option. Say, for example, we decide that users may 'View' attachments, but not 'Launch' (execute) or 'Detach' them. This would kill the risk from VBA macro viruses dead when sent as an attachment to a *Notes* client protected in this way. The *Lotus Notes* viewer can handle many file types (including *Microsoft Office* formats) and they do not run VBA macro code when the attachment is being viewed via the internal *Notes* viewer.

I am confident that I am not the only one who would like to see the following extension to the ECL implementation. It would be nice to see the ECLs extended to allow the optional blocking of attachments, so that these can only be 'Viewed' (in the in-built viewer), rather than 'Launched' (run) or 'Detached' (saved to disk).

The Bottom Line

Lotus Notes is, in my opinion, the package with the tightest and best-integrated security facilities of those groupware products available for use within most corporations. *Lotus Notes* security is multi-layered (with seven distinct layers in all) and in many ways can be likened to an onion – even if one layer of security is attacked and defeated there are other layers still to be bypassed.

The key to ensuring *Notes* is secured against targeted attacks is simply good, solid administration. Ensure that clients only have the minimum access rights necessary to perform their jobs. Proper use of the ECLs can minimize or neutralize such an attack.

Finally, there are products on the market that can be used to improve the level of virus protection in *Lotus Notes*. This is true for existing classes of virus and there are a few products which include features to help protect against *Lotus Notes*-specific threats. Scanning for viruses in *Notes*/*Domino* servers is required because otherwise *Notes* databases/email can become foxholes for viruses to hide out in, waiting to strike out again.

I hope I have given you a few things to think about as well as made you aware of some of the risks and solutions for *Lotus Notes*. More information can be found in a paper I presented at the 1999 *Virus Bulletin* conference in October. This paper is available at http://www.arachnophiliac.com cmindex.htm.