Viruses and Lotus Notes:- Have the Virus Writers Finally Met Their Match?

Martin Overton
*Chek*WARE

Version:- 1.01

Email: *ChekWARE@Cavalry.com*
WWW: ***http://www.arachnophiliac.com/cmindex.htm***
Tel: **+44 (0) 1403 241376**

51 Cook Road,
Horsham, West Sussex,
RH12 5GJ, United Kingdom.

Abstract:

Many companies are standardising on Lotus Notes/Domino as a groupware solution. With this move towards a standard groupware product and strategy, the risks from targeted attacks are increased.

Exactly how virus resistant is Lotus Notes and what unique threats do you need to be aware of, and more importantly, how do you counter them?

This paper aims to answer the above questions and the following questions, and offer advice that can be used in organisations that have or are planning to standardise on Lotus Notes/Domino.

- ***Has Lotus Notes reached the critical mass for virus writers to target it as they have the Microsoft Office components (Word, Excel, PowerPoint and Access)?***
- ***How will the virus writers approach this new vector for infection?***
- ***What are the threats from existing viruses, and how can these threats be minimised or eradicated in Lotus Notes?***
- ***What Notes specific threats (LotusScript, Buttons, Stored Forms, etc…) do I need to be aware of and what can be done to help minimise the potential threats?***
- ***What in-built security can be leveraged to help minimise the risks from virus attack?***
- ***How can encrypted mail be effectively used without risking viruses sneaking in through the outer-perimeter defences?***

This paper was written for, and presented at the 1999 Virus Bulletin conference at Vancouver, Canada on September 30th - October 1st 1999.

I would welcome any constructive feedback on this paper and it's content.
This paper will be updated from time to time.
(Martin Overton 5th October 1999)

Introduction

Although this is intended as a technical paper, where possible full and detailed explanations will be given so that any laypersons that may be reading this (*hopefully*) won't be too confused. Anyone with a reasonably technical or support background will find the main content of this paper understandable and maybe a little too basic. The malware[1] specific information and test results will be explained as clearly as possible within limited technical parameters of viral/malware nomenclature and related jargon.

As I began to research this paper I was astonished by the lack of testing of Lotus Notes with regard to viruses and other malware. I had noticed that there had been a few attempts by the virus authors to create a virus/worm that sent itself to others. The most successful before the end of January 1999 was Happy99 (*aka W32/Ska*). The relative success of this worm crystallised my own feelings that because of the standardisation of e-mail and *groupware (most companies had already decided to use Lotus Notes or Microsoft Exchange*) that very shortly we would see a targeted attack against one of these heavily adopted products.

Fig 1: W32/Ska aka Happy99 Firework Display When Run

No sooner had the abstract for this paper been accepted for this conference, than on the 26th of March 1999 Melissa hit the scene and was quickly hyped out of all proportion gaining almost mythical properties. It did almost exactly what I had feared, it was very tightly targeted at a groupware product, in this case Microsoft Exchange Server and Outlook 97/98/2000, talk about Deja Vu!

Then to cap[2] it all, in June along came W32/Explore.Zip… The stage was now set and the players had taken up their positions……

This paper is very focused on the traditional Lotus Notes functions (*E-Mail, Databases, and Replication*) rather than the Internet Web Server functions, as that side of Notes/Domino is a paper in itself, which I may cover at a later date.

Before jumping straight into the technical results, lets set the scene. So here goes, a potted history of Lotus Notes/Domino...

[1] My own current definition of malware is: "Code that causes unwanted effects: Such as viruses, Trojans (including Remote Access Trojans (RATS)), worms and the side-effects thereof. This could also be expanded to include Joke programs and related annoyances." I hope someone comes up with a definitive definition for this soon!

[2] No pun intended ;-)

What is Lotus Notes

Lotus Notes started life in 1989 as little more than a souped-up mail system. Indeed Notes caught the imagination of a few companies even before it was officially released…..

[NN] "*Lotus Notes was successful even before it released. The head of Price Waterhouse viewed a demo of Lotus Notes before the first release. He was so impressed by the product that he bought 10,000 copies of Notes. At that time, it was the largest PC sale of one product. As the first large Notes customer, Price Waterhouse predicted that Lotus Notes would transform the way we do business. They were right.*"

My own involvement with Lotus Notes started with this pre-release version and has continued to the present day.

Release 1.0

This is a quick summary of version 1.0….

[NN] *"The first release of Notes shipped in 1989. During the first year it was on the market, more than 35,000 copies of Notes were sold. With Notes, users could create and share information using personal computers and networks. This first release provided users with a graphical user interface, where they could manipulate information using a mouse. The Notes client required DOS 3.1 or OS/2. The Notes server required either DOS 3.1, 4.0, or OS/2."*

Onward and Upward

Since then and 4 major version numbers later, it has changed significantly. More and more functionality has been added without forgetting security; this has always been a part of its design and its appeal to large corporates, especially those in the financial sector.

Security features are part of the foundation that Notes is built on, unlike some other GroupWare vendors' products, that shall remain nameless, where security is seen as somebody else's problem.

A number of releases later and 4.5 arrived; suddenly Notes could be a web server….

Release 4.6

[NN] *"Notes Release 4.6 shipped in September 1997. By now Notes contains 5,694,358 lines of code. The focus of this release was personal information integration and management of content from Notes databases, Internet mail, and the Web. The developers added more Internet protocols to Notes.*
In 1996 Notes had an installed base of 10 million seats and a projected installed base of 18 million seats by the end of 1997. However, by the end of 1997 the install base was 20 million seats, doubling in only one short year."

Lotus/IBM describe Notes thus:

[NHL462] *"Lotus Notes® is a workgroup computing environment that helps people work together more effectively. With Notes™, people can work together regardless of platform or technical, organizational, or geographical boundaries. Notes-based information can be shared across any distance, at any time.*
Domino servers and Notes workstations
Notes consists of two primary programs: the Domino™ server and the Notes workstation.

The Domino server - a computer running OS/2®, Windows®, or UNIX® - provides services to Notes workstation users and other Domino servers including storage of shared databases and mail routing.

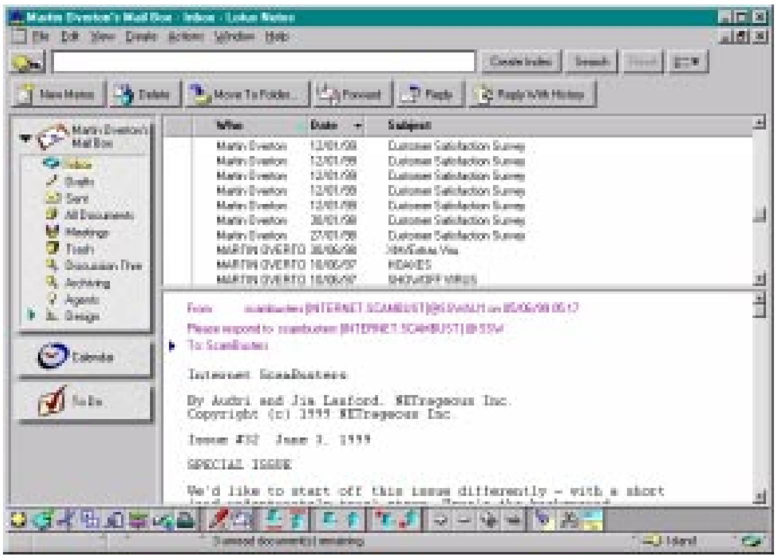
The Notes workstation - a computer running Windows, OS/2, Macintosh®, or UNIX system software - communicates with Domino servers so you can use shared databases and read and send mail.

Note *A Domino server is not the same as a file server. A file server is a computer that provides access to shared resources like printers and applications, and manages network activity."*

Notes consists of three distinct but overlapping functions, these are e-mail, databases and replication. A brief description of these functions appear below:

E-Mail

Fig 2: Notes Email Database Example



Who	Date	Subject
Martin Overton	12/01/99	Customer Satisfaction Survey
Martin Overton	12/01/99	Customer Satisfaction Survey
Martin Overton	12/01/99	Customer Satisfaction Survey
Martin Overton	12/01/99	Customer Satisfaction Survey
Martin Overton	12/01/99	Customer Satisfaction Survey
Martin Overton	30/01/98	Customer Satisfaction Survey
Martin Overton	27/01/98	Customer Satisfaction Survey
MARTIN OVERTO	30/06/98	[illegible] Virus
MARTIN OVERTO	16/06/97	HOAXES
MARTIN OVERTO	16/06/97	SHOWOFF VIRUS

From scambusters [INTERNET.SCAMBUST]@SSW... on 05/06/99 05:17
Please respond to: scambusters [INTERNET.SCAMBUST]@SSW
To: ScamBusters

```
Internet ScamBusters

By Audri and Jim Lanford. NETrageous Inc.
Copyright (c) 1999 NETrageous Inc.

Issue #32  June 3, 1999

SPECIAL ISSUE

We'd like to start off this issue differently - with a short
```

Notes mail enables you to communicate electronically with other Notes users as well as users of other e-mail products and platforms. You can exchange messages with people on the same network, or, if you're not connected to a network, such as when you are at home or at a away on business at a hotel, you can access your mail by dialing into a Notes servers using a modem and a telephone.

Notes mail supports sending and receiving of Notes mail, POP and SMTP mail, and version 5 now supports the fast growing IMAP protocol for mail. Notes 5 also supports Newsgroup (NNTP) discussions and now supports looking up of names and e-mail addresses using Internet directory services (LDAP) such as Bigfoot.

A Notes mail message is the same as any Notes document. For example, it allows full RTF formatting, you can change fonts and colors, add file attachments (version 5 supports MIME), and include tables, graphics, and links. Each Notes user has a mail database in which to store mail there messages and only they can read their mail (unless they have given sufficient rights to another party).

Notes is quickly adopting internet standards for mail and databases, in version 5 there is support for ActiveX (currently only in the Notes Browser), Java and JavaScript. Where will it end?

[WKC96] *"There are even more interesting developments on the horizon. The world is rushing headlong into Internet -based languages and systems like Java and Active-X - tying the world together into one huge seamless computing environment. What will viruses do in the new, global environment? It is likely that they will spread faster, and more widely, than even macro viruses do today."*

I believe we have already seen examples of early prototypes of these hypothesized new viruses, Trojans and other malware. Indeed the Internet appears to be the latest vector for viruses, and more and more virus authors appear to be equipping their creations with Internet smarts.

[IRBDD] "U*nless you have been asleep for the past few years, you will have noticed that the world is becoming increasingly network-centric. It is possible that this phenomenon is a reflection of marketing hyperbole, rather than reality. However, we prefer to believe that this time, just possibly, it is true."*

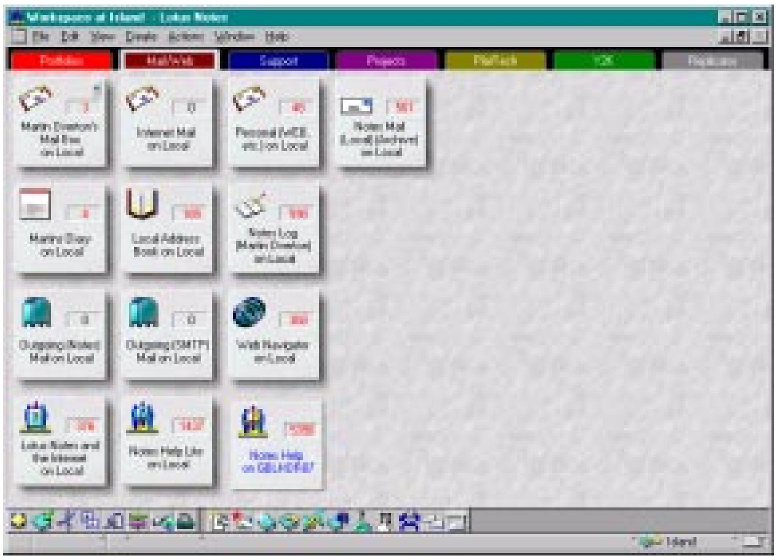
I concur with the above quote; the world is indeed becoming network-centric, at last. This is both a blessing and a curse!

Database Applications

A Notes database generally contains information about a single area of interest (or sometimes very diverse information), such as a help desk, a set of news items, or all the processes, forms, and policy for a company. In a nutshell: "*A Notes database is a single file containing multiple documents*".

These files (databases) can be personal (just on your own PC) or shared on a Notes server as a public resource or with access strictly controlled to a select few. Parts of the same database can even be public and others parts (forms and views) secured and only available to one or a number of clients.

Fig 3: Notes Desktop Showing Database Icons


Workspace at Island - Lotus Notes
File Edit View Create Actions Window Help
Portfolios
Mail/Web
Support
Projects
PlatTech
Y2K
Replicate
Martin Overton's Mail Box on Local
Internet Mail on Local
Personal (WEB, etc.) on Local
Notes Mail (Local) (Archive) on Local
Martins Diary on Local
Local Address Book on Local
Notes Log (Martin Overton) on Local
Outgoing (Notes) Mail on Local
Outgoing (SMTP) Mail on Local
Web Navigator on Local
Lotus Notes and the Internet on Local
Notes Help Lite on Local
Notes Help on GBLHDR87
Island

Lotus describes Notes databases below:

If you've worked with other database software, you may think of the items within a database as "records." You can think of a document within a Notes database as a record, but a Notes document is more sophisticated than a typical database record, containing rich text, pictures, objects, and many other types of information.

To read or write to a database, you first need to open it. You can use a database as long as you have the proper access. The first database you'll probably use is your mail database in which your e-mail messages are stored as documents.

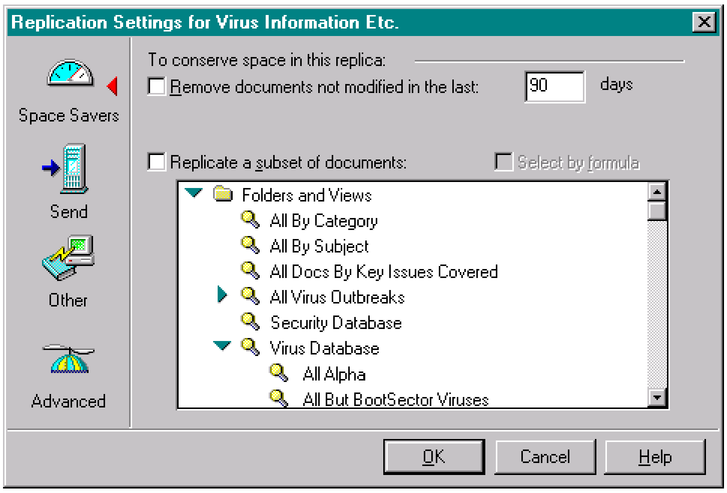
Most databases are stored on one or more Domino servers, accessible by many users. These are called shared databases. Databases that are used only by you and reside on your computer are called local databases.

You can also create a database from an existing template. Notes makes it easy for you to create a TeamRoom, Discussion, or a Personal Journal database.

Replication

This is the final part of the original Notes trio of groupware functions and this makes Notes extremely useful for sharing information between servers, be they in another part of a building or the other side of the world.

Fig 4: Notes Database Replication Settings Dialogue Box



Replication Settings for Virus Information Etc.

To conserve space in this replica:

□ Remove documents not modified in the last: 90 days

□ Replicate a subset of documents: □ Select by formula

- Folders and Views
  - All By Category
  - All By Subject
  - All Docs By Key Issues Covered
  - All Virus Outbreaks
  - Security Database
  - Virus Database
    - All Alpha
    - All But BootSector Viruses

Lotus describe replication as below:

Notes lets you keep multiple copies of a single file, called replicas, on multiple servers or workstations. This lets users on various networks in a variety of locations share the same information. A replica differs from a copy of a file, in that the original file and its replica have the same replica ID number. Replication is the process of sharing changes between replicas. When you replicate, Notes updates the replicas, copying changes from one to the other. Notes eventually makes all replicas identical. You can choose to replicate between replica copies, where both replicas send and receive updates, or only from one to the other.

You can also regularly schedule replication, or do it manually as needed. You can replicate between two servers or between a workstation, such as a laptop, and a server. When you schedule full replication, Notes makes all replicas identical over time.

Lotus Notes/Domino also offers Information sharing across Intranets and the Internet.

We will not cover this in this paper; maybe I will cover it in a future paper.

Has Lotus Notes reached the critical mass for virus writers to target it as they have the Microsoft Office components (Word, Excel, PowerPoint and Access)?

Lotus claim that Notes now has over [NN] 20,000,000 (million) users worldwide. Not quite up to the critical mass attained by the likes of MS Office at a claimed [MORK97] 40,000,000 (million) users across the globe, but Notes doubled its installed base in just one year. By now we could be looking at a minimum of 30,000,000 (million) licences in use.

So yes, Notes has now reached a required critical mass for it to be seen as a viable target by the virus writing community.

How will the virus writers approach this new vector for infection?

This is a difficult question to answer, for one, I'm not a virus writer and have no inclination to become one, and if I were would I have access to Lotus Notes, both client and server?

The answer is probably not, although evaluation versions are freely available on the Lotus website they are rather large 25MB for the client, and around 40MB for the server.

Even if I did have access to the server and client software, would I be prepared to invest the time to target Notes? What would be my motivation?

From my own research, I can honestly say that the effort involved would be quite considerable. Useful detailed information about the Notes security model is scarce and what is available is very patchy, mainly hinting at how the security model works, rather than giving details and examples. This is one area that Microsoft is more helpful; as we know to our cost, Microsoft offer very detailed information, good detailed examples and poor security to allow things to quickly spread with few or no impediments.

Well let's say they have got access to the client and server software, how would they approach trying to create a virus that could use Lotus Notes as an infection vector?

Firstly any virus writer would ideally need to fully understand the Notes security model, the macro languages supported and supposing that they would try to gain access to Notes via e-mail, as this is the most logical point of attempted entry into Notes, then they would need to decide how to target companies that they know use Notes.

To make their planned creation Internet aware it would need to be able to work on both Notes and via the common Internet e-mail standards, including MIME. Ideally it should be able to work seamlessly between Notes email, Exchange Server and the different flavours of Outlook. This is not a trivial task!

Certainly trying to infect other Notes databases would be far more difficult as any virus writer would either need to fully understand the Notes database file structure or have administrator (manager/designer) rights to the database they want to infect. This is far less likely to happen, unless the database security is very lax.

Allowing for all of the above, I believe that we will see Notes specific viruses/worms even if these creations only work on Notes/Domino servers and clients that have lax security standards.

Just like Microsoft Office files, it will prove to be too much of a challenge to ignore, even if it is only enough to prove their point and to show that the concept is possible[3]…..

[3] Intentional pun, this time!

What are the threats from existing viruses, and how can these threats be minimised or eradicated in Lotus Notes?

I will purposely not suggest anti-virus products during this section of this paper. I will however briefly cover anti-virus options later in this paper. This section purposely only covers the Notes specific functions that can be used to minimise known virus threats.

Threats

This can be generally summed up in a single word: ***ATTACHMENTS!***

This is not just a problem with e-mail but also with Notes documents stored in Notes databases. This is further compounded when you realise that many businesses use the replication facilities supported by Notes. This allows documents with infected attachments to be spread quite rapidly and because Notes uses a secure storage system, a standard on-access scanner only gets two chances to detect the intruder. The first being when an infected file is being attached to a Notes document and the other when the infected file is being launched or detached. The rest of the time, any infected attachments are as good as untouchable!

Also, remember that for a virus to be able to spread it has to have its code executed, such as when an Microsoft Office file loads and executes macro code assigned to auto macro functions, or when a screen saver is launched (it is after all only a renamed .EXE file with a few extra command line switches). The key is to get executed with or without user intervention! Few e-mail clients currently auto-run attachments, although there are ways to possibly achieve this via other message formats.

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 e-mail 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 [AVP1] PolyPoster and Caligula viruses.

Let's look at each major viral type in more detail.

Boot Sector Viruses

As they are, these cannot be easily spread as attachments, unless they are first generation sample stored in dropper, or are a multi-partile virus, infecting both executable files and system areas. Other possibilities are binary images of infected disks as attachments and scripts (DEBUG, etc.).

File Infectors

There are a number of sub types to this class, but to all intense purposes they can be clubbed together under a single umbrella. These are the executable infectors, that infect *.COM, *.EXE, *.DRV, *.SYS, *.SCR, etc.

This class of virus tends to make up the smallest segment of the outbreak reports, although this may well change as the virus writers adapt their creations to propagate successfully via the internet and the intranets that many large businesses now have in place. But these new creations are tending more towards being worms rather than viruses, so maybe I'm stretching the viral definition a bit thin.

Macro Viruses

This is our current greatest threat as the numbers of macro viruses are growing rapidly and as we all know documents and to a lesser extent spreadsheets, presentations and databases are passed intra-company and inter-company with little more than a second though. Although this culture is now starting to show signs of change, as many companies are starting to use PDF (Adobe Acrobat) for distributing documents instead, as this currently appears to be immune to virus attacks.

This aside, macro viruses make up around 80 percent of virus outbreaks reported each month. This trend does not seem to be showing any sign of reversing. Indeed a number of other vendors are now including VBA support in their products, such as in WordPerfect Office 2000 and Visio, so the possible number of targets is still increasing.

Some macro viruses are starting to use MAPI calls to ensure that they are spread more rapidly. This could equally be used to steal information and publicise it on the Internet or sent to an FTP server, as has already been demonstrated.

Worms

We have in the last year seen a resurgence of this class of threat. First with W32/Ska (aka Happy99) and then the appearance of Melissa[4] and finally W32/Explore.Zip.

Others

These include IRC scripts, Scrap objects (.SHS), etc.

[4] Melissa is a Macro virus with Worm-like properties in that is sends itself to others when the payload is supported (and triggered) on the current infected host system.

Solutions?

Notes offers a few options to help to minimise the threat from the existing classes of viruses. I will cover these briefly below, and cover these Notes functions in more detail later in this paper.

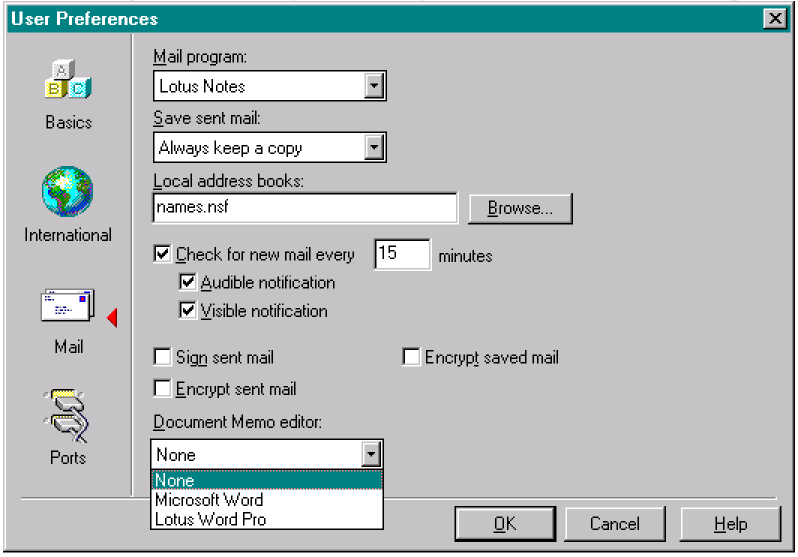
Macro Viruses

Let's cover this first as it covers the largest percentage of outbreaks each month [JAN99].

Well, currently you can't stop attached infected OLE compound files from being launched by a users intervention (loaded into Word, Excel, etc.) What you can do is:

1. Encourage the use the VIEW option on the attachment dialogue will allow you to read the Microsoft Office File without running any macros or VBA within the document or spreadsheet, etc.

Fig 5: User Preferences Dialogue Showing Document Memo Editor Options



User Preferences

Mail program: Lotus Notes

Save sent mail: Always keep a copy

Local address books: names.nsf

☑ Check for new mail every 15 minutes

☑ Audible notification

☑ Visible notification

☐ Sign sent mail

☐ Encrypt saved mail

☐ Encrypt sent mail

Document Memo editor: None

2. Ensure that the default Document Memo Editor is set to None, rather than Microsoft Word or Lotus WordPro.

3. Encourage the use of portable document formats that can't contain Macros or VBA code, such as Adobe Acrobat. I would have suggested Rich Text Format (RTF) but this can easily be subverted (as shown by Cap[5]) and therefore unless you are prepared to inspect the file format with a hex or ASCII editor you cannot be sure that the file really is an RTF file, and even then please be aware that although macros are stripped any embedded objects (*that may contain viral content*) are not.[NF99].

[5] WM/Cap, WM97/Cap, etc.

File Infectors

Apart from banning executable attachments (*.COM, *.EXE, etc.) there is little more that you can do to currently reduce the risk of file infecting viruses of this type. But lets put this into some perspective, this risk accounts for around 5% [JAN99] of reported virus outbreaks each month. This does not mean that this in a non-threat but that it needs to be taken in context against the preponderance of macro viruses.

Boot Sector Viruses

Disk images are not generally passed around, but this risk, although small needs to be understood. Monthly prevalence tables indicate that these average around 10% [JAN99] of all virus outbreaks.

Worms

We appear to be seeing a resurgence of file type malware. W32/Ska (aka Happy99) and W32/Explore.Zip are examples of this new threat. There seems to be little that Notes 4.6 security features can do about them. In fact the former appears to have caused the reports of file-infecting virus outbreaks to jump to over 16% in April of 1999 [APR99] and we may well see a similar jump in June and Julys figures.

Others

Again there is not a lot that Notes own security features can offer to counter these threats.

But all is not lost, all will be revealed later in the paper….

What Notes specific threats (LotusScript, Buttons, Stored Forms, etc…) do I need to be aware of and what can be done to help minimise the potential threats?

I will purposely not suggest anti-virus products during this section of this paper. I will however briefly cover anti-virus options later in this paper.

Threats

Let's have a quick look at the threats that are unique to Lotus Notes and its environment. 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 Trojan Horses, possible Denial of Service attacks and Mail Bombs.

Trojans

To do any damage, Trojan horses, unlike mail-bombs, first required an action from the user. This is not to say that they are any less dangerous, or that they are less likely to be activated.

This is now no longer true with the power of Notes functions and scripting languages in version 4.5 or later; simply opening (reading) or previewing a Notes e-mail or document (sent from another Notes client) can launch an attachment or run code.

The features that can be used to create Trojan horses are everyday Notes elements familiar to the user, and consequently they will be used without a second thought. Because the user recognises no difference the damage or payload may go unnoticed by the victim.

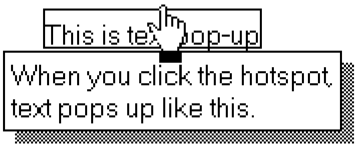
In this danger-area, the range of possibilities open to the sender is just as broad: Attached files (programs) can be detached and launched with severe consequences, and this can be achieved quite invisibly.

The main Notes features that are open to abuse in this way are:

- ***Buttons***
- ***Hotspots (popups and action hotspots)***

Since the arrival of Notes Version 4.x, the second of these are a particular danger because version 4 also allows the use of @Commands[6]. Up until this point, popups could only be used to display help-text, as of version 4.5 or later you can now attach more than just Notes formulae to Action Hotspots; this can include LotusScript, JavaScript and Simple Actions.

Fig 6: Example of a Hotspot (popup)



This is text pop-up

When you click the hotspot, text pops up like this.

This could equally be running a script behind the scenes and can be executed via clicking or on-mouse-over events

[JC99] **Examples:**

1. *Buttons which select all or a large number of documents and submit a delete or forward request.*

2. *Buttons which, for instance, try to erase your hard disk or various files (and can actually succeed!).*

3. *Action hotspots with similar functions.*

Mail Bombs

The term *mail-bomb* is applied here to a Lotus Notes feature, which is inherently *good*, but like most useful but powerful functions it is being deliberately misused for detrimental purposes. Mail-bombs differ from the *Trojan horses* in that they trigger as they are accessed by the user without any intervention being required.

There are currently two main types of mail-bomb:

- Stored forms
- Self-launching OLE objects

These two types are particularly effective when used in combination with each other.

The stored forms option will *force* a document, and this applies to E-mail too, into a stored form by saving (and sending) that stored form with the document.

From the technical programming angle a *computed for display* type field can also be used in a form to initiate a pre-defined string of events, these can of course be quite benign or quite devastating depending on the author's intent.

It's fair to say though that this design element can't do an awful lot of damage because the range of *dangerous* Notes @Functions available in this type of field is quite limited - at least up until Version 4.0.

Mail-bombs are the most pernicious threat because unlike viruses, they cannot be detected by conventional means.

[6] Notes formula function.

Worse still - a good many mail-bombs will go off with (virtually) no intervention from the user. Merely opening one up can be enough. This may be as simple as viewing or pre-viewing[7] the e-mail.

[JC99] ***Examples:***

1. *Floods of mail can be unleashed (@MailSend) on opening one document. The damage caused internally may be minimal. However, if the mail deluge is directed outside (Compuserve, WorldCom) e.g. via modems, the financial impact could be considerable.*

2. *Self-launching OLE objects can theoretically achieve almost complete infiltration of the system. This could even mean theft of user-ids complete with their passwords, or theft of other sensitive information. In other words, the entire Notes system is effectively exposed.*

LotusScript

In many ways this is very similar to Microsoft's VBA, this similarity I believe will soon give rise to LotusScript viruses, Trojans and Worms.

Indeed I have already seen a sample of a LotusScript routine that can delete a file when triggered. I also have a sample of a LotusScript routine that launches an external executable when the document is opened or previewed. It is very possible that LotusScript could become the *Achilles heal* of Notes, as VBA is to Microsoft Office applications. Or maybe not as we will see later.

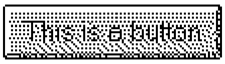
[SOPH99] JavaScript

In theory, JavaScript is risk-free because it has no access to, and indeed no concept of files on your hard drive, memory management and other system resources. Client-side JavaScript more-or-less exists for dynamic web-page content generation. There were some loopholes in earlier JavaScript implementations (allowing things like malicious emails to be sent out under someone's identity), but apparently these have been addressed in the current JavaScript 1.2 (as supported in IE4 and Netscape Navigator 4).

Buttons

These can be used to achieve any function that the author intended, as long as he has the rights to perform these actions and as long as the intended victim clicks on the button stored in the document or email.

Fig 7: Example of a Button



Stored Forms

This should be turned off, as otherwise mail bombs are a distinct possibility. This can be achieved at database level (via the ACL[8]) or via the ECLs[9] (Both Administrators and Client).

Stored forms were first introduced in Notes version 2 and have since become considered a security threat. Many administrators insist on turning these off at database level. However as of version 4.5 or later this feature can be controlled via the ECLs instead.

Stored forms can contain Formulae, JavaScript or LotusScript that can be triggered when the e-mail is opened or even *previewed.*

[7] In the Notes preview window
[8] Access Control List
[9] Execution Control Lists

OLE
Lotus define OLE below:

"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
Lotus define formulas below:

"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".

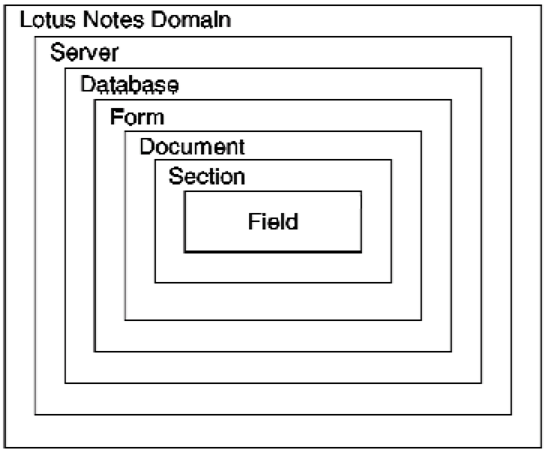
Field Formulas
See Formulas (Above)

What in-built security can be leveraged to help minimise the risks from virus attack?

Let us now quickly cover Notes own security model.

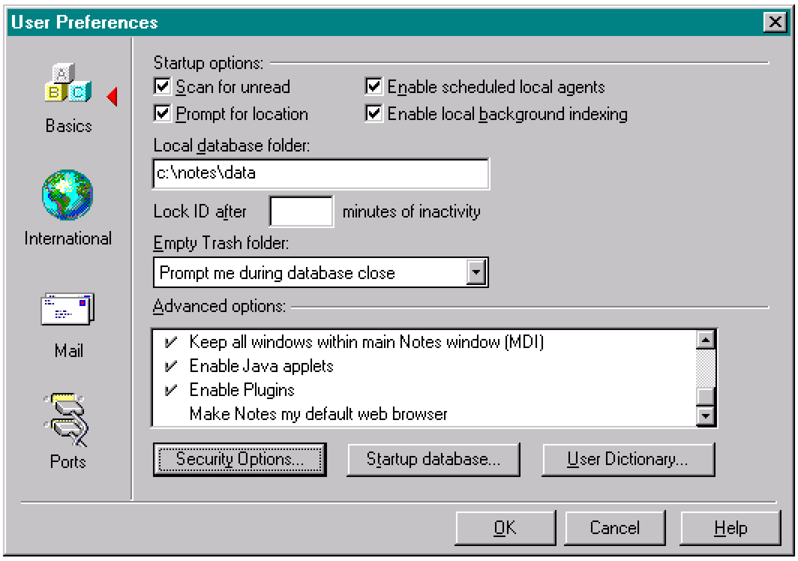
[NN] *"Perhaps one of the most powerful selling points of Notes is the depth and breadth of its security features. It has more flexible and effective security than any mail product, database, or Web server while still managing to promote the sharing of information. It can do this because the security features are so comprehensive that you can make information widely available and still be sure that no information will be released to the wrong people. Notes security allows administrators to control who has access to servers, directories, databases, documents and even fields. Notes was designed to meet the security requirements of major banks around the world, and even the CIA is using it!"*

Fig 8: Notes Seven Layers of Security



Access control facilities within Lotus Notes can be looked at as seven layers from the outside in. The outside layer is simply the security involved in having any access to the Notes structure. The innermost layer involves security at the field level within a Lotus Notes document.

Fig 9: Notes User Preferences Dialogue Box



Startup options:

☑ Scan for unread
☑ Enable scheduled local agents
☑ Prompt for location
☑ Enable local background indexing

Local database folder: c:\notes\data

Lock ID after ___ minutes of inactivity

Empty Trash folder: Prompt me during database close

Advanced options:

✓ Keep all windows within main Notes window (MDI)
✓ Enable Java applets
✓ Enable Plugins
Make Notes my default web browser

Clicking on the 'Security Options' button gives you access to the client ECL

ACLs and ECLs

These are the main components of database, server and client security.

Let's look at the options for the ACL for a Notes database first.

Access Control Lists

These are linked directly to databases and user access rights to them. The key here is that these should only allow those that need access to a database the minimum rights they need to do their job. By default the database should be set to No Access.

[NHL5] After users or other servers gain access to a server, they will want some level of access to the data held by that server. The database layer of the Domino security model and the layers below that deal with data access, each layer providing more granular control than its predecessor. In fact, the access controls mirror the way that Domino stores and presents data:

- Database access

At the heart of the system lie Domino databases. The records in a database are actually documents that have usually been entered by a user or administrator. Database access control facilities, therefore, provide the broadest control over who can do what to data on a Domino server.

Access Level	**Privileges**	**When to assign...**
Manager	Can modify ACL settings, encrypt a database for local security, modify replication settings, and delete a database--tasks permitted by no other access level. Managers can also perform all tasks allowed by other access levels.	Notes requires each database to have at least one Manager. It's best to assign two people with Manager access to a database in case one manager is absent.
Designer	Can modify all database design elements (fields, forms, views, public agents, the database icon, Using This Database document and About This Database document), can modify replication formulas, and can create a full text index. Designers can also perform all tasks allowed by lower access levels.	Assign to the original designer of a database or to a user responsible for updating the design after a database is in use.
Editor	Can create documents and edit all documents, including those created by others.	Assign to a user responsible for maintaining all data in a database.
Author	Can create documents and edit documents they create.	Assign when you want to allow users to contribute to a database but not edit documents created by others. When possible, use Author access rather than Editor access to reduce Replication or Save Conflicts.
Reader	Can read documents in a database but cannot create or edit documents.	Assign to users who must be able to read the contents of a reference database such as a company policies database.
Depositor	Can create documents but can't see any documents in the database views, even the documents they create.	Assign to allow users to contribute to a mail-in database or to a database used as a ballot box.
No access	Cannot access the database.	Assign as the default access to prevent most users from accessing a confidential database.

- Form access

Documents are not free-form text, but are in fact filled-in forms. When designing forms, you can use form access controls to specify who has access to the contents of a database in more detail than you can by using the database access controls.

- Document access

Once a form has been filled in to create a document, the owner of the document can further restrict access to it. To what degree this is allowed depends on controls within the form from which the document is created.

- Section access

Many documents contain data of varying sensitivity. In practice this means that you want to prevent certain users from updating or possibly even from reading parts of the document, but you want other users to have full access.
One way to achieve this is to divide the form into sections and apply section access controls to it.

- Field access

This is the most granular form of data access control. It allows you to control access to individual fields on a form or document. In addition to specifying user access, field access controls can limit the treatment that data receives when it is transmitted or stored.

ECL (Execution Control List)

[GT99] Execution control lists were first introduced in Lotus Notes R4 and are akin to virus behaviour blockers.

[NHL5] In the past Notes has provided little protection from the actions of code that the user knows nothing about[10], for example viruses and Trojan horses. With the new ECL feature a user can specify which digital signatures are required in order to perform certain actions on their workstation. If an action is not permitted or the signature is not trusted, a message will display informing the user that an unauthorized action is about to occur. The user can then decide to go ahead with that action if they so wish, or to stop it.

The Notes administrator can set the ECL to a standard by using the Edit Execution Control List action in the Public Address Book.

ECLs allow or deny access to the Notes environment and also to external functions, such as the ability to launch a program. If properly used ECLs should render many Notes specific threats impotent.

However, you must understand that ECLs rely on trust mechanisms that operate via digital signatures. This model maybe flawed, as it relies on the premise that the action will be allowed if the document was signed by a trusted source as safe. [PD97] Paul Ducklin summed up the problem with signing files thus: "*From an anti-virus perspective this means that 'signed' is being misinterpreted as 'uninfected'*"[11].

This (digital signing) is rather a good solution for limiting directed attacks, such as mail-bombs and Trojans.

I believe that this approach will ultimately fail when it is applied to viruses, as the trusted source may, or may not be aware that the Notes function they are signing is actually infected (either accidentally or on purpose). Finally, there is a small chance that the signature could be forged or even circumvented[12].

[10] Dave Chess kindly pointed out that there was an obscure NOTES.INI (in version 3.0) setting that could be set to disable the ability of formulae and scripts to do anything dangerous at all before the advent of ECLs.

[11] This is my interpretation of his statement, my apologies to Paul Ducklin if I have taken this out of context.

[12] Although the mechanisms used are very secure.

Furthermore ECLs can only (currently) be used to limit the actions of Notes functions, such as Formulae, Scripts (such as LotusScript and JavaScript), Stored Forms, etc. These actions can include the launching of attachments and any other programmed payload.

ECLs have no effect whatsoever on attachments (such as Microsoft Office files, Executable files, etc.) that are not linked to Notes functions. This means that if an Office document is attached to a Notes document the user can *launch/view/detach* it as normal without Notes flagging any potential risks that the attachment may contain. They can happily run infected attachments!

There are two distinct ECL types used in a Notes/Domino GroupWare environment the option are the same for both; these are:

Administrator ECL
This ECL controls what can be run on the server and is used as the default when clients are installed.
Client ECL
This ECL controls what can be run on the client system.

ECL Settings
This is Lotus's description of ECLs

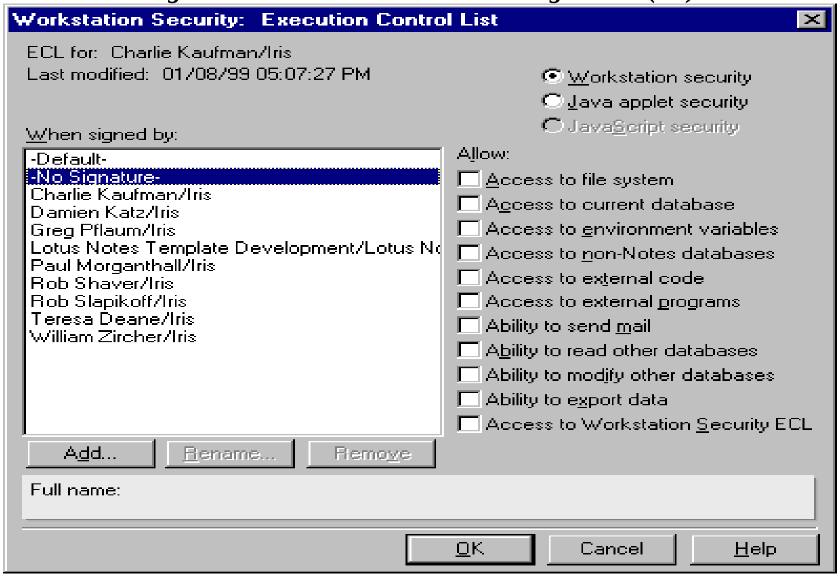
By default, no scripts or formulas, whether signed or unsigned, can execute on your workstation without displaying a warning message. However, scripts or formulas run from any database created with a template that ships with Notes are signed "Lotus Notes Template Development/Lotus Notes", and this signature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

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

> ***Note*** *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

Fig 10: Execution Control List Dialogue Box (R5)



Workstation Security: Execution Control List

ECL for: Charlie Kaufman/Iris
Last modified: 01/08/99 05:07:27 PM

● Workstation security
○ Java applet security
○ JavaScript security

When signed by:
-Default-
-No Signature-
Charlie Kaufman/Iris
Damien Katz/Iris
Greg Pflaum/Iris
Lotus Notes Template Development/Lotus N
Paul Morganthall/Iris
Rob Shaver/Iris
Rob Slapikoff/Iris
Teresa Deane/Iris
William Zircher/Iris

Allow:
□ Access to file system
□ Access to current database
□ Access to environment variables
□ Access to non-Notes databases
□ Access to external code
□ Access to external programs
□ Ability to send mail
□ Ability to read other databases
□ Ability to modify other databases
□ Ability to export data
□ Access to Workstation Security ECL

Full name:

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.

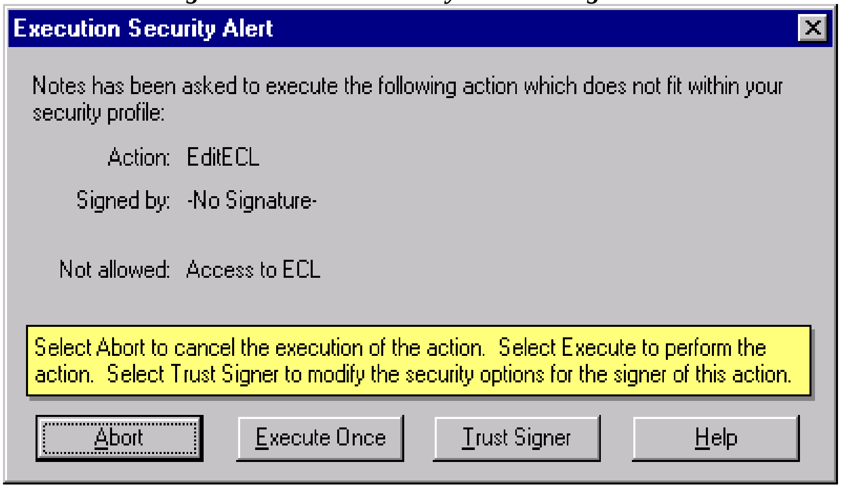
As you can see the *key* here is that the ECL settings only affect agents, scripts and macro function included in databases, forms and fields.

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

Get the feeling that you could be looking at the macro warning dialogue 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[13]?

Fig 11: Execution Security Alert Dialogue Box


Execution Security Alert

Notes has been asked to execute the following action which does not fit within your security profile:

Action: EditECL

Signed by: -No Signature-

Not allowed: Access to ECL

Select Abort to cancel the execution of the action. Select Execute to perform the action. Select Trust Signer to modify the security options for the signer of this action.

Interestingly in Version 5 of Notes Lotus added the following support to ECLs:

[NHL5] **Note** You can also restrict access to signed Java applets and JavaScript applications. In the Execution Control List, select either "Java applet security" or "JavaScript security," and go through the list of access options you want to give to each signer.

And also…

[NHL5] **Note** A user who shares a computer with others can set up his or her own ECL. ECLs are unique to each person's User ID.

Yet they still offer no option to restrict attachment launch/detach by users themselves. Why? Surely offering such a facility would ultimately help to negate some of the risks posed by sharing Office files[14].

Let's look at this proposed option

[13] This risk can be removed by the administrator locking the clients access to change their ECL.
[14] Of course I'm playing Devils Advocate here. No current GroupWare/Office Suite offers anywhere near the level of security that Notes/Domino offers. Nevertheless, I would still like to see this feature added.

Let's say 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 Notes viewer can handle many file types (see the table below) and they don't run VBA macro code when the attachment is viewed via the internal Notes viewer.

Ami Pro® (.SAM)
Ami Draw (.SDW)
Bitmap (.BMP)
CompuServe GIF
Computer Graphics Metafile (.CGM)
Executable file (.EXE)
Freelance Graphics (.PRE)
JPEG, TIFF (.TIF, .JPG)
Lotus 1-2-3 for Windows (.WK3, .WK4)
Lotus 1-2-3 for OS/2 (.WG2)
Lotus PIC
Macintosh PICT and PICT2
Microsoft Excel (.XL*)
Microsoft PowerPoint 4.x, 7.0 (.PPT)
Microsoft Word for Windows 6.0 (.DOC)
Rich-Text Format (.RTF)
Text (.TXT)
Windows Metafile (.WMF)
Word for Macintosh 4.0, 5.0
WordPerfect 5.x, 6.x (.DOC, .WPD)
WordPerfect for Macintosh 2.0, 3.0
WordPerfect Graphic 2.0
ZIP file (.ZIP)

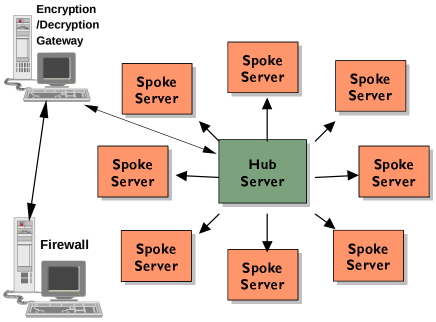
Unfortunately the list of supported files is quite limited, although for many companies it probably is quite sufficient as it supports many common file formats that are exchanged.

How can encrypted mail be effectively used without risking viruses sneaking in through the outer-perimeter defences?

Encryption has its uses, and indeed is becoming more widely used in many large companies for not only privacy but also non-repudiation. Unfortunately it is also widely used just *'because its there'.*

If you are insistent upon its use, then setup encryption/decryption gateways downstream of the Notes server that is running the virus detection software. This approach would be suitable where you wish to encrypt data passing between offices over public networks. To enable this a single company-wide key would be required. Other keys can be used where appropriate and these should be treated as rare exceptions as they can otherwise become the weak link in your defences.

Fig 11: Hub and Spoke Network Model With Encryption/Decryption Gateway



What 3rd Party Tools Can I Use To Improve My Cover?

Let's have a brief look at anti-virus tools that can be used to improve the virus resistance of Lotus Notes and viruses that can be propagated via Notes as attachments.

Notes Specific and Standard Virus Threats

Workstation

Where possible on-access scanners should be installed to detect and prevent infection from PC viruses. A few virus scanners are now starting to offer protection from new threats, such as Java, ActiveX and VBScript based malware.

There is little that the current virus scanning offerings can do against Notes specific threats. Though I believe that this will start to change soon as attacks against GroupWare products become more common.

Notes Server

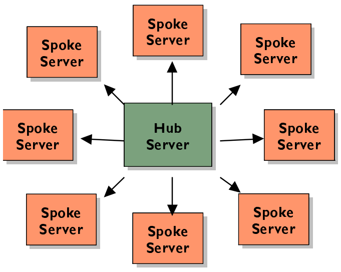
There are now a number of companies offering anti-virus solutions for Lotus Notes/Domino. Some just focus on existing PC virus threats (we'll call this Type X) and others offer both existing PC virus detection as well as Notes specific threat detection (we'll call this Type Y). Both have their place in a corporate strategy.

In many corporates, mail hubs (central servers) are used to simplify distribution and scanning of email and Notes databases. This is an ideal situation to be in, as central administration and protection of this hub is possible. These hubs are frequently used not just to link-up Notes servers but also often act as mail gateways to the Internet and beyond.

A few of these Type Y products allow the use of multiple virus scanners, and this again is an ideal solution for corporate use as it offers some overlap.

These hub servers (as if you are an international company, you will tend to have at least one per geographic region) should be configured to run the Type Y protection, and the spoke (or satellite) servers should be setup to run the Type X protection.

Fig 12: Hub and Spoke Network Model



This model ensures that any mail or database replicas destined for another server have to pass through the hub server and therefore are checked for PC viruses as well as Notes specific threats. The only slight risk is from mail and database replicas that stay on the local spoke server, attachment will still be virus scanned but Notes specific threats will be missed.

Conclusions

Although there are no Notes specific viruses at the time of writing, it is just a matter of time before they appear. There are reported cases of Trojans for Notes.

As Richard Ford stated [RF1] "More functionality may seem like a good thing, but it is always worth considering how these extra functions might be put to a less than glorious purpose."

Encryption has its uses but if you are insistent upon its use, setup encryption/decryption gateways downstream of the Notes server that is running the virus detection software.

The key to ensuring Notes is secured against targeted attacks is simply good, solid administration. Ensure that clients only have the minimum access rights to perform their jobs. Proper use of the ECLs and ACL can minimise or neutralise such an attack[15].

Virus scanning of Notes/Domino servers is required, as otherwise Notes databases can become foxholes for viruses to hide out in, waiting to strike out once more.

Use a hub and spoke topology for Notes/Domino servers as this offers the easiest solution to administer for many companies.

[15] Unless it's an inside job.

Appendices

Virus Bulletin Virus Prevalence Tables

VB Prevalence Table April 1999		
Multi-partite	9	0.2%
Boot	143	2.9%
Macro	4059	80.4%
File	842	16.7%
Total	5053	100%

VB Prevalence Table January 1999		
Multi-partite	18	0.90%
Boot	240	11.98%
Macro	1656	82.63%
File	90	4.49%
Total	2004	100.00%

Usenet Postings

```
From: "Nick FitzGerald" <nick@virus-l.demon.co.uk>
Subject: Re: what COMMON files are infectable?
References: <7kp1qg$149$1@news8.svr.pol.co.uk>
<FDry5G.BsK@cix.compulink.co.uk>
Organization: Personal account
Message-ID: <01bebf48$f07802e0$f61eb584@mobilenick>
X-Newsreader: Microsoft Internet News 4.70.1155
Newsgroups: alt.comp.virus
Date: Fri, 25 Jun 1999 05:31:01 -0400
Path: insnet.net!news-lond.gip.net!news-
peer.gip.net!news.gsl.net!gip.net!newsfeed.cwix.com!151.142.223.51!WCG!arl-
news-svc-3.compuserve.com!news-master.compuserve.com!nntp-
nih2naaf.prod2.compuserve.com
Lines: 127
Xref: insnet.net alt.comp.virus:69049

"Graham Cluley" <sophos@cix.compulink.co.uk> wrote:

> kriptick@kriptick.freeserve.co.ukSPAMOFF (Krip Tick) wrote:
<<snip>>
> > affected & frequency in the wild. I’ve read that there
> > are now viruses affecting .HLP, .MDB & .PPT & maybe other
> > more esoteric file types but is there really much chance of
> > coming across one of these?
>
> It depends on how often you transfer those kind of file types around your
> organization (and indeed outside your organization).  Most companies
> are more likely to transfer Word documents and Excel spreadsheets
> regularly than Access databases and Powerpoint presentations.  And that’s
> probably why Word and Excel viruses are more common.

Whilst I agree in general with Graham, he does not state the real case
(or at least, not strongly enough).  The "trouble" with listing the file
extensions to be wary of is now analogous to the older problem of of
how to meaningfully answer a question of the form "Is ABCDEFGH.EXE
infected?" which in turn hinges off problems hanging around "Is
ABCDEFGH.EXE a Trojan?".

It is dangerously misleading, as it suggests to the naive reader (which
is the intended audience for Krip Tick’s musings) that "all other
extensions are OK".

> Working out what is possible executable from its file extension is
> becoming more and more difficult, and the distinction between
> executable and data is becoming more fuzzy.  EXE, COM, BAT, SYS, VXD,
DLL,
> FON, SCR, OVL (overlays), MDB, DOC, DOT, XLS, PPT, is a good list for
> starters.
```

And RTF, HTM[L], VBS, and others. Oh, not to mention files with no extension whatsoever, as recent spates of O97M/Tristate have shown!

If you are concerned about more than just viruses -- the broader spectrum of malware -- then you cannot meaningfully extend this list much without it becoming laughably large. If what Krip Tick is looking for is a pithy statement of the form "Avoid files of type [????] if received as Email", then s/he should just write "Avoid attachments". Whilst not all attachments are potentially harmful, most "typical users" have no adequate method for deciding which actual attachments *are* harmful. If you are prepared to stake your security precautions on the ill-informed judgments of rank amateurs, let them have their Email attachments -- if not, block them...

Trend Micro (makers of antivirus and other "computer security" products) were reportedly hit by ExploreZip for exactly this reason -- they leave (maybe "left" now??) such decisions to such typically technically able people as upper management.

> But it really isn’t the way to do it I’m afraid. For instance, a DOC file
> can be saved with any extension (for example, .DOG or .CV or even .TXT)
> and can be just as infective.

Indeed.

And although much over-hyped (due to lack of understanding of the real issue when it was first announced last year) *any* file can be "wrapped" and therefore "hidden" in SHS files, which can then produce nasty surprises when double-clicked on Win32 machines.

And worse still, MS is working at making file extensions *not important* (as they aren’t under MacOS). With slow but increasing moves to "extension less file typing" *now* is NOT a good time to start teaching your charges that .DOC files sould be avoided if from unknown/untrusted sources... The important thing, as Graham (and others) allude to is what is in the file. What kind of file is it internally and does *that* have virusable potentional. If the answer to the latter question is yes, then avoid it.

Now, does anyone else see the "problem" here??

Yes -- it requires quite some degree of skill and understanding **in the end user* to make the "correct" decision in any given case. Why is this? At least partly, it is because MS included "executable code" into what "should be" *data files*.

If "data files" and "executable content" could be kept separate, then things could, potentially, be much easier...

> The digital signatures incorporated into the new Microsoft Office 2000 are
> not the solution either (find out why in the paper by my colleague Paul
> Ducklin at http://www.sophos.com)

Indeed -- this is a **very important** point. Do **NOT** be sold on the idea that the digital signing technology in Office 2000 will impact the virus problem greatly. All it takes is someone you "trust" to have become infected and s/he could be sending you signed, infected documents.

> Macro viruses have been seen in Microsoft Word documents, Excel
> spreadsheets, Access databases, Powerpoint presentations, and Corel
> Draw err.. drawings. I also hear that the new WordPerfect 2000 is going

Errrr -- no.

At the moment, Corel SCRIPT viruses are limited to the files containing the ccode that is interpreted/run. that is, to Corel SCRIPT files. For the (increasingly misdirected) extension-minded, that is .CSC files

> to incorporate VBA which means it will be possible to have viruses in them
> too.

Indeed. Such viruses will (if/when) be contained in drawing files (.CDR ?) and so on...

> My advice would be to install a decent on-access scanner (like
> InterCheck from Sophos :)) and let that do all the worrying for you.
> InterCheck includes intelligent file recognition which means it doesn’t
> care if your users have distributed a file with a strange extension, it
> will still get zapped.

With the increasing moves to extensionlessness (or, at least, the lessening of importance of file extensions on MS’s Windows platforms) this is ever-better advice.

--
Nick FitzGerald

AVP Encyclopedia (http://www.avp.ch)

Macro.Word.Agent (aka PolyPoster)

This is a polymorphic and stealth Word macro virus. It contains one macro "AutoOpen" and replicates on opening documents . The virus deletes the following menu items:
Tools/Macro, Tools/Customize, File/Templates, Format/Style.
The mutation (polymorphic) engine, depending on the random counter, inserts random comments into random positions into the virus code and renames some virus variables with random selected name. This engine is "slow" because it is executed only if, on infection, the current seconds are 23 or 45 only. As a result, in 97% of cases the polymorphic engine will not be executed and the "child" infector will have the same code as "parent" one.

Depending on the random counter the virus sends a copy of current document to Internet news-groups, so to spread itself the virus uses global networks. It also can be a reason of confident information disclosing, if it is a part of document that is sent to Internet.

To post documents to Internet the virus executed the news client AGENT.EXE, selects one of the news-groups (see the list below) and sends a message to there. The message has one of several possible Subjects (see the list below), the text "WM/Agent by Lord Natas" continued with random selected characters and attached infected document.

The list of news-groups looks like follows:

alt.aol-sucks
alt.binaries.cracks
alt.binaries.pictures.erotica
alt.binaries.warez.ibm-pc
alt.conspiracy
alt.drugs.pot
alt.fan.hanson
alt.flame
alt.hacker
alt.sex
alt.sex.necrophilia
alt.sex.stories
alt.sex.zoophilia
alt.windows95
alt.sex.passwords
alt.binaries.warez
alt.binaries.sounds.mp3
alt.comp.virus
alt.2600
alt.2600.hackerz
alt.skinheads
alt.sex.babies
alt.sex.bondage

Subjects are:

Free XXX Passwords
Check this out!
Official WaReZ site list
Easy Money!
My first fuck by Todd
Hanson rulez!
Warez mailing list details
Crackz mailing list details
Learn to hack!
Attn: All k3wl h4ck3rz
Important Info
New Virus Alert!
Serial Number List!
Official mp3 site list
Elite XXX site list
New erotic story
Important Princess Diana Info
Important Monica Lewinsky Info
How to find child pornography
Cable TV descrambler instructions!
Kewl N64 Emulator & MP3 sites

References

[GT99] Gregory Tetrault, Anti-Virus Solutions for Lotus Domino - White Paper - Sybari Software 1999

[WKC96] Steve White, Jeff Kephart and David Chess, The Changing Ecology of Computer Viruses - Proceedings of the Sixth (1996) International Virus Bulletin Conference pp201

[NN] Lotus Web Site [Notes.net]

[NH462] Lotus Notes Help Lite - Notes 4.6.2

[NHL5] Lotus Notes Help Lite - Notes 5.0a

[IRB-DD] IBM Red Book - The Domino Defense: Security in Lotus Notes and the Internet

[MORK97] Microsoft Office 97 Resource Kit.

[JAN99] Virus Bulletin Prevalence List - January 1999

[JC99] John Carol - UIT - UK Vendor of WatchDog

[SOPH99] Sophos GroupWare Developer

[PD97] Paul Ducklin, Anti-Virus Research: What's Over The Next Hill - Proceedings of the Seventh (1997) Virus Bulletin International Conference pp11

[RF1] Richard Ford, Why Viruses Are and Always Will be a Problem (http://ncsa.com.knowledge/research/d.htm)

[JAN99] Virus Bulletin Virus Prevalence Table January 1999 (see appendices)

[APR99] Virus Bulletin Virus Prevalence Table April 1999 (see appendices)

[AVP1] Description of PolyPoster from the AVP virus encyclopaedia (see appendices)

[NF99] Nick Fitzgerald - posting to alt.comp.virus (see appendices)