GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

GSEC Practical assignment version 1.4b option 1.

Sergei Freiman

Norton AntiVirus Corporate Edition 7.6 – keep virus definitions up to date.

Introduction

Good protection of corporate computer systems against viruses relies on many components: security policies and their enforcement, user community awareness of virus' threat, careful selection of the most suitable product and its implementation to name a few. Among these components the task of keeping virus definitions files and scanning engine up to date is, without doubt, the prime concern of administrators responsible for the protection of corporate networks against viruses. Antivirus software is useless and may give a false feeling of protection without current virus signatures.
"…antivirus companies are cataloging 200-400 new malicious programs a month…" [1]
Modern antivirus software products are highly sophisticated systems with a wealth of customizable features allowing administrators to tune them according to their specific requirements. I will look at different methods updating Symantec's Norton Antivirus Corporate Edition 7.6 (NAVCE) installations with regularly published virus definitions, product updates, and patches. LiveUpdate and Virus Definition Transport Method are native ways to keep updated virus signatures files in NAVCE 7.6 and require minimum configuration. Intelligent Updater is another method and requires manual input or execution of batch files. Definition Updater is a mechanism designed to transfer the updates using a corporate e-mail system and is very useful for unmanaged clients or users on the road. The way that NAVCE client maintains its local copy of virus definitions may vary depending on its type: a server, a desktop workstation, or a mobile laptop. The intent of this paper is to show the reader how these methods deliver new virus signatures to clients and how they can be configured depending on their type.

I assume from the reader an understanding of such terms as Master Primary, Primary, Secondary, and Parent Servers, managed and unmanaged clients, Symantec System Center and refer to Chapters 1 and 2 of the Norton Antivirus Corporate Edition 7.5 Implementation Guide [2] for a basic familiarity with Norton AntiVirus Corporate Edition concepts. I have limited my discussion to Windows platform only and have not covered other server and client platforms such as Netware, Mac OS, or Unix.

Symantec is taking care

Symantec publishes product updates and new virus definitions files on its web page http://securityresponse.symantec.com/. There are two forms: Intelligent

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Updater executable and LiveUpdate package. Intelligent Updater executable only contains virus definitions. It is published on a daily basis Monday through Friday. On the other hand LiveUpdate package contains new virus definitions and in addition may contain product updates and patches. It is usually published every Wednesday. During a virus outbreak a LiveUpdate package can be published more often. Both Intelligent Updater executables and LiveUpdate packages have completed quality assurance testing. In the past, definitions in the form of Intelligent Updater were only available for download from FTP site. Although the definitions were tested, they were still considered to be beta definitions.

How it works

In a logical flow of a centralized process of delivering updates to NAVCE clients I distinguish two logical phases: during the first phase updates are delivered from Symantec to a corporate internal distribution point; during the second phase updates are delivered from that distribution point to NAV Servers and clients. The centralized process has many advantages. There are two reasons why clients should get updates from an internal distribution point. The first is security, the second is Internet link bandwidth efficient utilization. Instead of having dozens, hundreds, or, possibly, thousands of clients going to Symantec FTP or Web sites to download roughly 6.5M of data per host daily, only one host accomplishes this, greatly reducing bandwidth utilization and allowing more strict security settings on corporate firewalls and monitoring software.

Note: The LiveUpdate packages use a microdefs file allowing download of just modified portion of virus signatures files. The volume of transfer can be as small as 300K. But remember – LiveUpdate packages are published once a week.

Another advantage of using this two-step model is the possibility for an administrator to test new virus definition updates and, more importantly, products updates and patches in a lab environment. Only after they are approved, the new virus definitions, product updates, and patches may be posted for distribution for internal clients.

In the first phase two mechanisms may be used: Intelligent Updater and/or LiveUpdate. If we use the Intelligent Updater executable to get new definitions from Symantec, the internal distribution point is a Primary Master Server. If we use LiveUpdate, the point is an internal LiveUpdate Server or a Primary Master Server depending on how LiveUpdate is configured. Once updates have reached the Primary Master Server or the LiveUpdate Server, during the second phase they can be distributed to Master Servers of server groups, Secondary Servers, and clients. In order to do so and depending on the specific requirements use is made of different techniques. The techniques include LiveUpdate using an internal LiveUpdate Server, Intelligent Updater, Virus Transport Definition Method (VDTM), Definition Updater, and copying a Virus Database (.vdb) file from a protected server.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

First Phase

As I have pointed out in the preceding paragraphs there are two mechanisms which can be used to obtain updates from Symantec: LiveUpdate and Intelligent Updater. The mechanisms differ from one another in three following ways.

- The Intelligent Updater is published every day; the LiveUpdate package is published once a week.

- The Intelligent Updater delivers only new virus signatures; the LiveUpdate package delivers virus signatures, product updates and patches.

- Update using the Intelligent Updater is a push operation and can be scheduled to run as often as required; LiveUpdate is a pull operation when NAV Server or client connects to Symantec using internal scheduler and retrieves updates. With Symantec System Center the LiveUpdate can be scheduled to run on a daily, weekly, or monthly basis.

Now let's cover these two mechanisms in more detail.

Intelligent Updater.

Usage of this method provides us with the most current virus definitions as soon as they become available to the public. Intelligent Updater executable file is available for manual download from a Symantec web page http://securityresponse.symantec.com/avcenter/defs.download.html or from the Symantec FTP Server [4]. The name of the file to download is in the format yyyymmdd-xxx-x86.exe. The file is around 6.5MB, and it incrementally grows. After the download, the Intelligent Updater needs to be executed on a Primary Master Server. The execution will update the Primary Master Server itself and prepare all necessary files for further distribution down to all Master Servers of other server groups and to all Secondary Servers of its own group. A variable file name makes difficult usage of automated scripts, so Symantec created a special static folder [5], where the Intelligent Updater is always named **symcdefsx86.exe** and provided a script to automate the downloading process. "How to automatically update Norton AntiVirus Corporate Edition 7.x definitions without using LiveUpdate" [6]. The batch file **cegetter.bat** will run the ftp script **cescript.txt**, download Intelligent Updater, execute it in a silent mode, and copy necessary files. <PATH> is a location where a local installation of NAV monitors availability of new definitions. Unless the location of Program Files folder is specified differently, <PATH> = C:\Progra~1\NAV for NAV Servers and for Norton AntiVirus clients <PATH>= C:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5.

cegetter.bat

```
ftp -s:cescript.txt
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
"c:\temp\symcdefsx86.exe" /q /extract /vdb c:\temp
copy c:\temp\*.vdb <PATH>
del /q c:\temp\*.vdb
del /q "c:\temp\symcdefsx86.exe"
```

cescript.txt

```
open ftp.symantec.com
anonymous
nobody@spammer.com
cd public/english_us_canada/antivirus_definitions/norton_antivirus/static
lcd C:\temp
bin
hash
prompt
get symcdefsx86.exe
quit
```

The **cegetter.bat** batch file can be scheduled to run as often as required.

Intelligent Updater can be used to update just one Master Primary Server. The Primary Servers and all of the Secondary Servers will be consequently updated using the Virus Definition Transport Method (VDTM). They in turn will update their clients. Intelligent Updater can be used to update just one Parent Server and all its children. Or Intelligent Updater can be used to update an unmanaged client when run locally. Execution of Intelligent Updater applies all necessary changes.

LiveUpdate

The LiveUpdate utility is an integral part to many of Symantec's software lines including Norton AntiVirus Corporate Edition, Norton AntiVirus for Microsoft Exchange, Norton AntiVirus for Firewalls etc. Symantec uses the LiveUpdate utility to distribute updates and patches to users of its products. The utility connects to Symantec LiveUpdate Server on the Internet and downloads update packages and applies new definitions to all Symantec products installed on the computer on which it is running. The LiveUpdate execution can be initiated manually or scheduled.

As an alternative to going to the Internet, the LiveUpdate utility can be configured to connect to an internal LiveUpdate server to retrieve the update packages. This type of setup is called a Central LiveUpdate and requires a configuration of an internal LiveUpdate server with LiveUpdate Administration Utility (LUAdmin). LUAdmin retrieves definitions and updates for all specified Symantec products and downloads them into a designated directory. An administrator shares the directory using one method of his or her choice: Web server, FTP server, or UNC share.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

As shown on Figure 1, during the first phase, the Master Primary Server can retrieve updates directly from the Symantec LiveUpdate Server, or from an internal LiveUpdate Server.

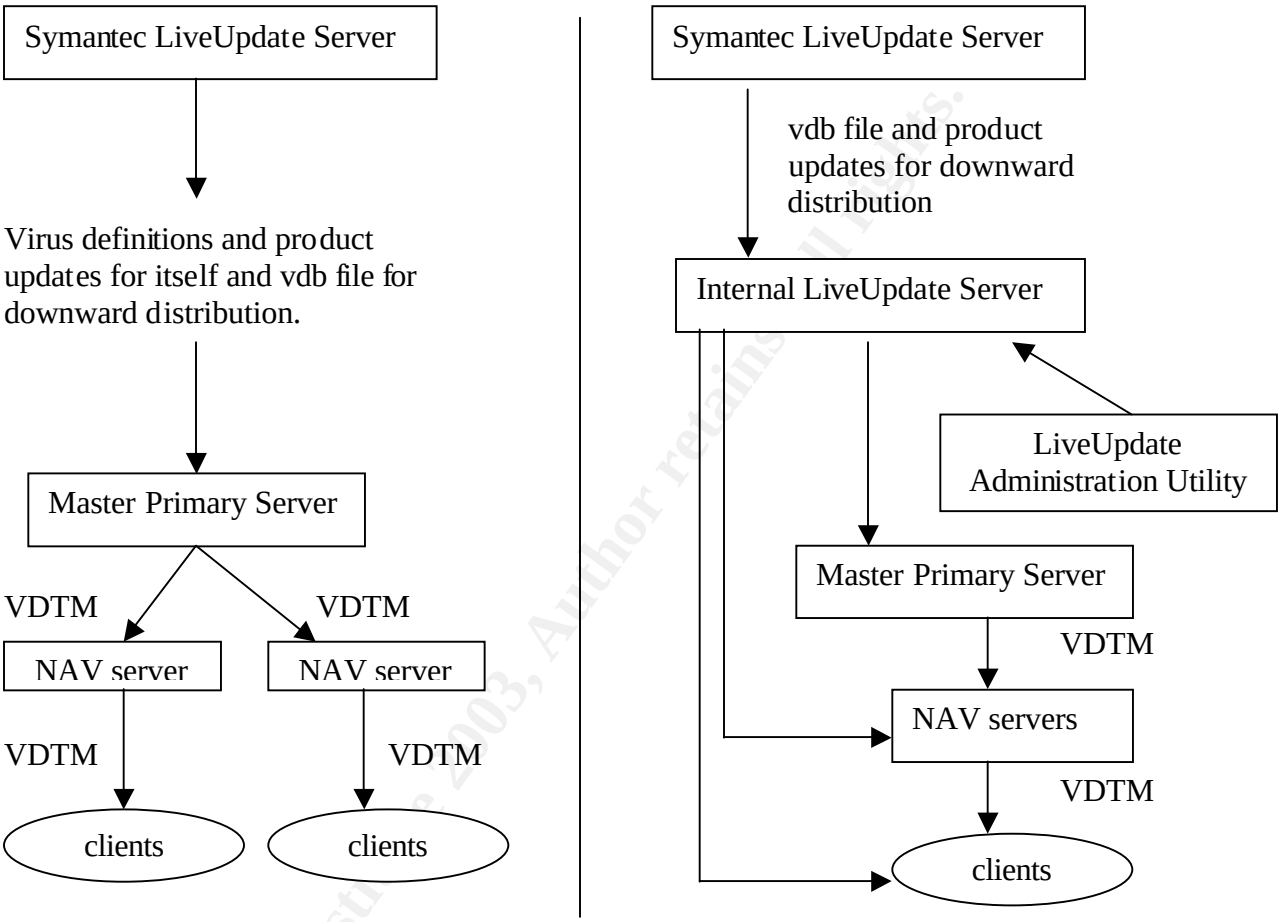


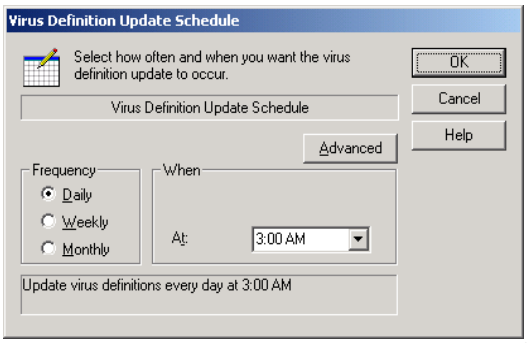
Figure 1. Updates using an internal LiveUpdate server versus straight connection to Symantec LiveUpdate Server.

When the Primary Master Server connects to Symantec LiveUpdate Server directly, only virus definitions in the form of vdb file are available for client and server community using VDTM. In the second case virus definitions AND product updates are available for distribution. By default a LiveUpdate utility on a Primary Master Server is configured to connect to the Symantec LiveUpdate Server; the only required configuration parameter is a frequency of retrievals. The frequency of retrievals can be set using Symantec System Center:

Open Symantec System Center
Right-click on the Primary Master Server
Select All tasks -> Norton AntiVirus -> Virus Definition Manager

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Keep the option “Update the Primary Server of this Server Group only”
Click Configure button, then Schedule button.



As it can be seen from the screen shot, the LiveUpdate can be scheduled to run as often as once a day, which is appropriate in most circumstances. If the administrator decides that more frequent execution of LiveUpdate is desirable, he or she can schedule an execution of vpdn_lu.exe located in Program Files\nav folder. For a silent execution use /s option.

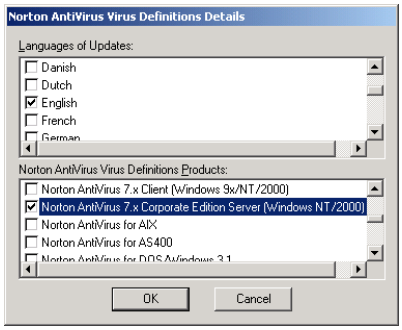
When the administrator chooses to distribute updates through an internal LiveUpdate Server, he or she is required:

- Install and configure a LiveUpdate Administrator utility
- Configure one of three types of internal shared storage: Web, FTP, or LAN File Server
- Point the Primary Master Server to retrieve LiveUpdate packages from that storage instead of Symantec LiveUpdate Server.

LiveUpdate Administration Utility

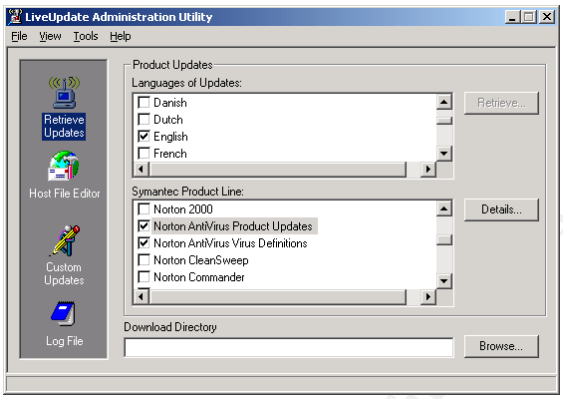
The LiveUpdate Administration Utility can be installed on Windows NT or Windows 2000 workstations or servers. If it is installed on the computer running the NAVCE Server, it can then be scheduled using Symantec System Center. The LiveUpdate Administration Utility has three main functions:

- Which products updates to take from Symantec:



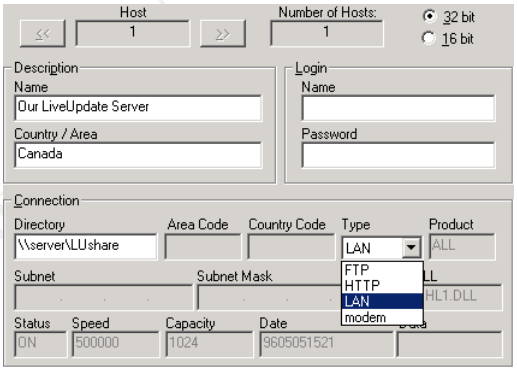
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Where to put them on the network



- Modify a standard default.hst file

  Basically, an hst file points LiveUpdate Utility to a LiveUpdate Server. For managed clients the real location of a LiveUpdate Server overwrites a default one by settings controlled by their Parent Server, and, originally by a Master Primary Server. For unmanaged clients, or when Symantec System Center is not used, a customized liveupdt.hst file is required.



Using Host File Editor a customized Liveupdt.hst has following fields:

- Description fields are arbitrary.

- Login Name and Password fields are used only when connecting to Web or FTP servers.

- Connection fields contains UNC path when LAN File Server is used or URL or IP address and subnet mask when connecting to Web or FTP servers.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The customized liveupdt.hst file needs to be saved into the C:\Program Files\Symantec\LiveUpdate folder on each unmanaged client or client who's settings are not controlled by Symantec System Center. Furthermore copy to the same folder the S32luhl1.dll file from C:\Program Files\LiveUpdate Administration Utility folder on the computer where LUAdmin Utility is installed. When a client runs LiveUpdate Utility version 1.6 and up, the liveupdt.hst file is converted into the file Settings.LiveUpdate and the original file liveupdt.hst is deleted.

When LiveUpdate Utility runs in unattended mode under Local System account , the process will fail because Local System account does not have rights to access network resources. As a workaround Symantec suggests to enable and create null session shares. [7] In the Windows registry under the subkey HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionShares add the name of the shared folder used for LiveUpdate downloads. But first we must explicitly enable null session access on shares. Under the key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA create a new value RestrictAnonymous, Data Type: REG_DWORD, Value: 0.

If we configure a shared resource in this manner, the resource is not secure. Microsoft does not recommend this configuration. [8] Enabled null session shares option is on the fifth place on the SANS/FBI list of Top 20 Vulnerabilities. [9]

Second Phase

During the second phase updates are delivered from an internal corporate distribution point to Master Servers of server groups, Secondary Servers and, finally to NAVCE clients. Norton AntiVirus Corporate Edition 7.6 has a number of methods to deliver updates to end clients. Different clients might have to use different techniques depending on their location on the network and availability of the connection to the network. To make a right choice let's look at how these methods differ from each other.

Virus Definition Transport Method

VDTM is a fully automated process with minimal required configuration. Once a Master Primary Server was updated using LiveUpdate or Intelligent Updater, it starts a push operation to other NAV Servers on the network. The NAV servers in their turn begin immediately to push the new definitions to their clients. VDTM employs a virus definition file with a .vdb extension. The vdb file contains a full package of virus definitions and VDTM passes the file from a Primary Server to all Secondary Servers into a folder …\Program Files\NAV. Secondary Server extracts the file and places definitions into a folder …\Program Files\Common Files\Symantec Shared\VirusDefs\INCOMING. DefWatch service monitors the INCOMING folder and as soon as new definitions appear in that folder the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

service picks them up and updates the local installation of Norton AntiVirus. After the update, the INCOMING folder is cleaned. For NAV CE clients, their Parent Servers passes the vdb file into the C:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5 folder. The file is then extracted into the INCOMING folder and a Defwatch service updates a local client NAV installation. VDTM method has two disadvantages:

- Full definition vdb file is always transferred to servers and clients. The size of vdb file is around 4.5M.

- VDTM transfers virus signatures only.

LiveUpdate

There is a clear advantage of updating clients from an internal LiveUpdate Server over using VDTM: LiveUpdate packages are transferred to clients in a form of microdefs files which are smaller in size (around 500K) then a full vdb file because they contain only modified portion of virus definitions. This relates to NAVCE clients only, NAV Servers always get a full vdb file. In a WAN environment this advantage fades out because each site has to have its own LiveUpdate Server to avoid the transfer of these short microdefs files over a WAN link, thus greatly increasing an administrative burden. In a WAN environment VDTM should be used to transfer the virus signature updates to clients because a vdb file is transferred between a Master Server and a Secondary Server only once and use LiveUpdate for product updates and patches.

NAVCE clients inherit LiveUpdate settings from their Parent Server. It means that as soon as the Master Primary Server is pointed to an internal LiveUpdate Server, all Primary Servers will also retrieve update packages from it.

Copying a .vdb file from a protected server.

When a client computer is unmanaged and does not have a connection to the Internet, a simple file copy operation can keep this client updated. Every NAV server has a VPHOME share. The VPHOME share contains a vdb file required for a client update. The vdb file needs to be copied into the C:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5 folder on the client computer. The rest of the process will be done automatically. The vdb file will be extracted and necessary changes will be applied. The vdb file itself is not needed for NAV operation and can be discarded. The Norton AntiVirus client keeps the five last vdb files and deletes all older versions. An administrator can also download the latest vdb file from Symantec FTP site ftp://ftp.symantec.com/public/english_us_canada/antivirus_definitions/norton_antivirus/vdb/ and share it in a folder of his or her choice. If the downloaded file has a

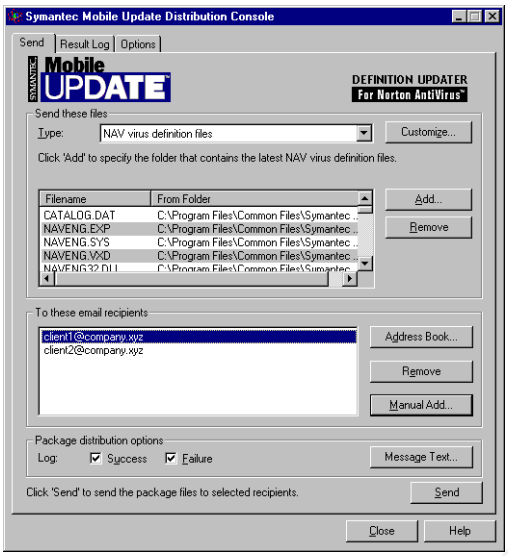
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

name in a form similar to **vdb144405.vdb.zip**, remove the .zip extension while keeping .vdb

Definition Updater

It works with Norton Antivirus to automatically update virus definitions using corporate e-mail system. It applies updates fast and transparently to unmanaged clients or mobile users who are frequently on the road and have access to a corporate e-mail system. Definition Updater segments the virus definitions files into small chunks and sends them in a sequence of email messages. The Definition Updater system has two components: a Distribution Console – an administrator's tool, and a client Agent that is installed on every NAV protected computer we plan to send updates to. An administrator selects the files that need to be distributed to clients for updating, and sends them to e-mail addresses of these clients. Definition Updater breaks these files into chunks of a specified length and sends them each in a separate e-mail message. When messages are received, the Agent component of Definition Updater automatically reassembles the files, and updates the virus definitions on a client computer. The Definition Updater is not a standard part of the Norton AntiVirus Corporate Edition 7.6, and it needs to be installed separately. First, the Distribution Console has to be installed. The location of the Setup program is on CD1 in the PRODMGMT\NOSUPRT\MOBILEUP folder. The Distribution Console requires a local installation of Norton AntiVirus and a dedicated e-mail account. After the Distribution Console is installed the Definition Updater Agent can be distributed to clients. To ensure that the Agent distributed to clients and the Distribution Console itself is up to date, an administrator can use the LiveUpdate feature. The installation of the Agent is a two step process: first, the Agent installation executable is sent to users via e-mail using the Distribution Console, second, users run the Agent's executable and configure e-mail and monitoring options. The Agent installation package can not be segmented, it is sent as attachment in one e-mail message. The size of the attachment depends on a type of e-mail software used by client, for Outlook 97/98/2000 and Outlook Express it is 2M. Before using the Distribution Console an administrator configures the console to use an e-mail account from which the update messages will be sent and where result log files will be received, and the maximum attachment size. The default size is 4096K. When new virus signature files are available, the administrator determines which files are new in that distribution and includes them in package to be sent, and chooses recipients to whom the updates will be sent to.
The administrator can review the Result Log sent by Agent after update process, and in case of failure resend the package to failed clients.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



From the users' point of view Definition Updater functions almost transparently. The Agent detects update messages during the next period of monitoring the mailbox, reassembles them, and applies changes. The Agent then deletes messages and puts an update status message into the user's outbox to be sent to the Distribution Console's Result Log. No user interaction is required when update messages are waiting in the Inbox. An administrator has to instruct users not to open or delete the update messages, or move them using Inbox Assistant Rules, otherwise the Agent will fail updating virus definitions.

Norton AntiVirus Corporate Edition Implementation Guide [10] by Symantec Corporation was used as a primary resource for this paper.

References:

1. Roger A. Grimes. *Malicious Mobile Code: Virus Protection for Windows.* O'Reilly & Associates. ISBN 156592682X. August 2001. page 3.

2. Norton Antivirus Corporate Edition 7.5 Implementation Guide URL: http://www.symantec.com/techsupp/enterprise/products/nav/nav-75-ce/manuals.html

3. How to update virus definitions for Norton Antivirus Corporate Edition. URL: http://service1.symantec.com/SUPPORT/ent-security.nsf/3d2a1f71c5a003348525680f006426be/ab3b224da335e9f388256a22002726c4?OpenDocument

4. Location of Intelligent Updater download ftp folder URL:ftp://ftp.symantec.com/public/english_us_canada/antivirus_definitions/norton_antivirus/

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

5. Location of Intelligent Updater with static name symcdefsx86.exe
URL:ftp://ftp.symantec.com/public/english_us_canada/antivirus_definitions/norton_antivirus/static/

6. How to automatically update Norton AntiVirus Corporate Edition 7.x definitions without using LiveUpdate
URL: http://service1.symantec.com/SUPPORT/ent-security.nsf/3d2a1f71c5a003348525680f006426be/d89b2365520f4bbf88256a220026a5f3?OpenDocument

7. How to create a null session share
URL: http://service1.symantec.com/SUPPORT/ent-security.nsf/c31d80c3f677ecab88256b67003221d8/85c0660ffcd24f9688256a2200272af2?OpenDocument

8. Enable Null Session Shares on a Windows 2000-Based Computer.
URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q289655

9. The Twenty Most Critical Internet Security Vulnerabilities
URL: http://www.sans.org/top20/#W5

10. Norton Antivirus Corporate Edition Implementation Guide version 7.6. Symantec Corporation, 2001

© SANS Institute 2003, Author retains full rights.