Global Information Assurance Certification Paper

The gap between a New virus and a New Signature.

Cavanna Santiago
GIAC Security Essentials Certification (GSEC)
Practical Version 1.4b option 1
July 2003

1) Contents

2) Abstract

Organizations protect themselves from the threat of viruses by implementing antivirus solutions in their workstations, servers, messaging services and the perimeter.

Currently, Computer Associates, Network Associates, Symantec and Trend Micro represent approximately 75 % of the market share **(1)** and they generally present very good characteristics of central administration, handling of alerts, signature updating and early response as against new viruses.

However, computer networks keep getting infected with viruses at an alarming rate and frequency, that is to say, the chosen solution is not sufficient by itself and it requires supplementary measures in order to reduce the risk of infection as against these new viruses.

This paper analyzes four solutions, the last solutions available from each vendor, the signature updating procedures offered and the average response time as against new viruses, and it provides recommendations on the measures to be taken in order to minimize the risk of infection by new viruses while the new firms are developed. The main objective of this article is to show that any antivirus vendors update solution is similar but not enough to stop the virus problem.

The products assessed are the following:**(2)**

	Management:	Servers.	Workstation.
Computer Associates.	eTrust Antivirus 7.0	eTrust Antivirus 7.0	eTrust Antivirus 7.0
Network Associates	ePolicy Orchestrator versions 2.5	VirusScan Enterprise v7.0	VirusScan Enterprise v7.0
Symantec	Symantec System Center.	Symantec Antivirus Corporate Edition Client. 8.1	Symantec Antivirus Corporate Edition Client. 8.1
Trend Micro	Trend Micro Control Manager 2.5	ServerProtec 5.5	OfficeScan 5.5

This paper just analyzes workstation and server platforms, and the reason of that is that antivirus software at gateways level is a perimeter solution, which was not widely adopted in the region.

Workstations and servers anti-virus software are more easily updated than gateway products. Gateways anti-virus software is supplement with perimeter security products such as Firewall & IDS and I will not touch this issue at this time.

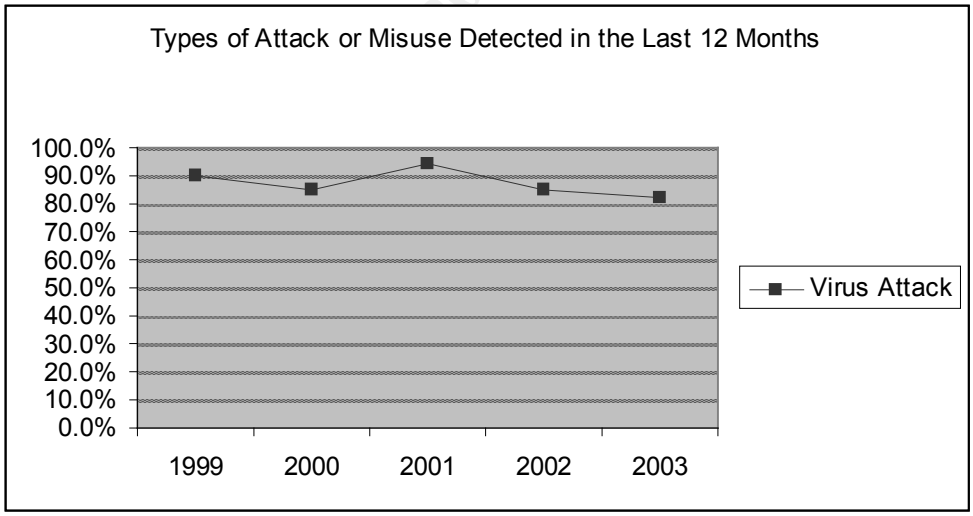
3) Introduction:

For the eighth consecutive year, the organization "**Computer Security Institute",** prepared a report called **"CSI/FBI COMPUTER CRIME AND SECURITY SURVEY" (3),** in relation to which curiously, and despite the technological distance separating Latin America from North America, I see coherence as to a particular point.

Viruses periodically infect most organizations although they have antivirus solutions, which I believe, they are in the last generation Antivirus solutions and they do properly implemented. (Here in Latin America as well as North America),

The following table shows recently values (2003) of reported incidents (by organizations, which are part of the investigation). The percentage of companies that have suffered viruses' attacks is remarkable, as it is the fact that these values have not decreased with the passing of years, the put into operation of better management practices, or more powerful virus detection products.

Types of Attack or Misuse Detected in the Last 12 Months (by percent)			
Year	Virus Attack	Quantity of Respondents	Percentage of Respondents
1999	90.0%	460	88.0%
2000	85.0%	583	90.0%
2001	94.0%	484	91.0%
2002	85.0%	455	90.0%
2003	82.0%	490	92.0%

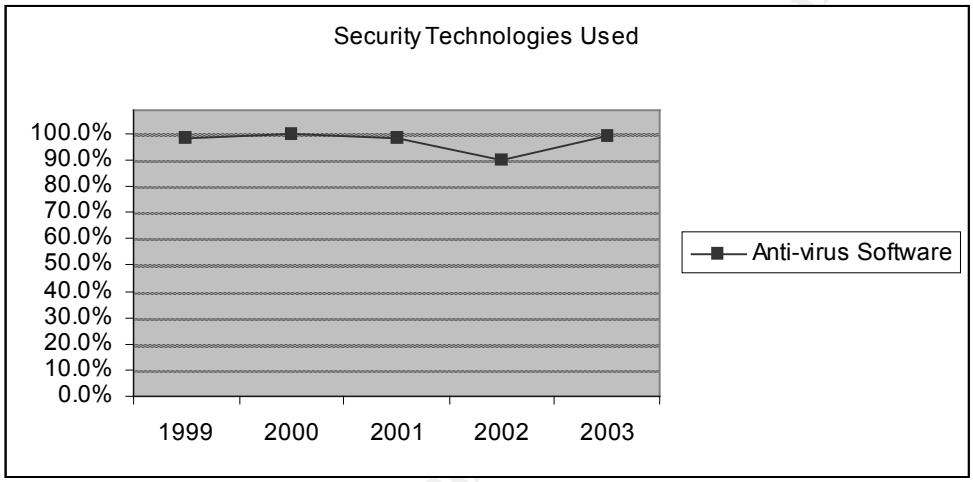


The statistics and the graphics that are presented up, contain information taken of: "FBI2003.pdf, 2003 CSI/FBI Computer Crime and Security Survey (page 6) http://www.gocsi.com/forms/fbi/pdf.html.

The same survey shows the percentage of companies that have anti-virus technology. It does not specify how new it is (year of acquisition or version), whether it is updated, well managed or if it encompasses all the possible points

of entrance of information and viruses. However, the antivirus solution has the most important percentage of adoption to the security technology.

Security Technologies Used			
Year	Anti-virus Software	Quantity of Respondents	Percentage of Respondents
1999	98.0%	501	96.0%
2000	100.0%	629	97.0%
2001	98.0%	530	99.0%
2002	90.0%	500	99.0%
2003	99.0%	525	99.0%



The statistics and the graphics that are presented up, contain information taken of: "FBI2003.pdf, 2003 CSI/FBI Computer Crime and Security Survey (page 5) http://www.gocsi.com/forms/fbi/pdf.html.

There is a high percentage of responsibility for infections caused by new viruses, which an organization could suffer at its workstations and servers.

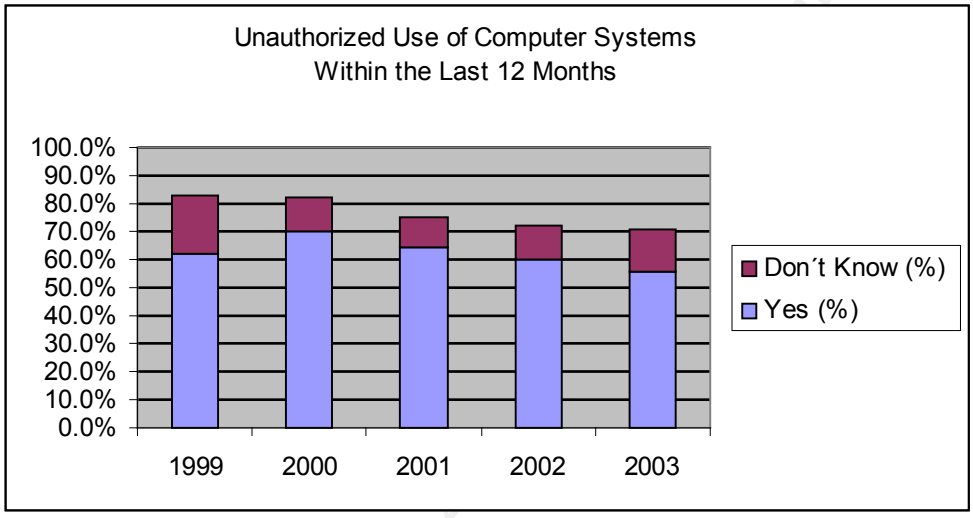
The computer security policies and the organization's culture may or may not facilitate the implementation of preventive security tasks but unfortunately statistics show a very slow progress in this direction.

Particularly in South America, the direct impression derived from contact with many organizations (state-owned and private organizations), is that the need to develop and implement formal security policies as a basis for the continuity of the operations or business, is just being putting forward.

The unauthorized use of systems, which includes software implementation by the user without the approval of the systems area, or personal use of the systems, browsing through internet sites which are not related to the specific work of the user, etc. This, together with the lack of tools or control practices over the workstations; shows how difficult may be to keep the equipment updated in

terms of the last Antivirus and fixes updates (many of them consisting of corrections or improvements in security aspects) for each of the software packages, which has been installed.

Unauthorized Use of Computer Systems Within the Last 12 Months					
Year	Yes (%)	Don´t Know (%)	Total (%)	Quantity of Respondents	Percentage of Respondents
1999	62.0%	21.0%	83.0%	512	98.0%
2000	70.0%	12.0%	82.0%	585	91.0%
2001	64.0%	11.0%	75.0%	532	99.6%
2002	60.0%	12.0%	72.0%	481	96.0%
2003	56.0%	15.0%	71.0%	524	99.0%



The statistics and the graphics that are presented up, contain information taken of: "FBI2003.pdf, 2003 CSI/FBI Computer Crime and Security Survey (page 10) http://www.gocsi.com/forms/fbi/pdf.html.

4) Analysis of the response time of the Anti-virus solutions vendors as against new viruses.

How can the Antivirus vendors could get the newest virus in for analyze proposes?

The new viruses detection procedure begins when a user of the solution detects an unusual activity at his workstation because of the infection by a virus not recognized.

At this moment, a sample of such virus has sent to the research center of the respective vendor.

All the solutions allow the user to send the infected-files, manually or automatically, supplying information of the environment (operating system,

product version, engine date and signature). It may be sent through http/s or through e-mail (compressed and encrypted).

The final goal of vendor is that the largest possible number of suspicious files reaches the laboratory, so that they can identify, remove or include within the list of new detected viruses.

Usually, the vendor will send a temporary signature update to the client, which has supplied the sample-infected file, which will contain the instructions for its effective detection and removal (if possible). Meanwhile, it will test the other applications using the same signature updates in order to determine their compatibility.

At this moment, and depending on the intrinsic danger posed by the new virus, the usual time for the release of new signatures will be awaited, within which it will be possible to include other definitions of equal or lesser risk. This update will be available for the users of the solution to be downloaded and distributed to the workstations.

In case of a very dangerous virus, the update will be immediately released, and a newsletter or alert will be issued in order to inform the solution managers of the existence of such virus.

Annex 1 contains a comparative chart of the several vendors, in relation to the 15 recently viruses. The names used for their identification, and the date on which they were included within the new definitions.

The criteria used in the selection of these viruses are the following:

- They are included within the list of New Viruses, which was published, in the respective websites, during the first week of July 2003.
- The name given by the other vendors to the same virus was expressly specified.
- During its particular analysis, there was no doubt to the fact that it was the same virus (because of its behavior and consequences)

It is important to mention the following:

- Each vendor depends primarily on the suspicious files sent by their customers.
- Each vendor will name a new virus according to their own criteria for names.
- Not all viruses appearing as “New” in each update are documented within the encyclopedia that the vendor itself offers on line to their customers.
- It is not always easy to relate the names of a vendor to those of another; therefore, it is very difficult to determine whether all vendors detect the same virus.

From the comparison performed, the following conclusions may arise:

- There is not a clear winner in terms of new signature updates (particularly, as this comparison is so difficult in terms of the criteria available, we believe that each vendor's average time of response is similar)
- The creation of a new virus definition may take several days beyond the average time (in accordance with the experience recorded), putting the assets of its organization at risk.
- The average time of new signatures ranges from 1.6 days (Symantec) to 3.3 days (Network Associates). That is why in addition to its own internal update architecture, its network will probably be unprotected as against a new virus for a longer time than the time that it usually takes for a low-risk virus to spread (48-72 hs), and this is, finally, the experience recorded by **CSI/FBI 2003**
- In case of appearance of a new virus, which is very dangerous due to its impact and propagation method, the vendors usually, frees one or several Updates on that same day on which it was detected.

5) <u>Analysis of the signature updating procedures</u>

Basically, the idea is that if in order to detect a new virus we must apply a signature update (detection pattern) or an engine and signature update in each workstation, we must have the policy, procedures and tools in order to do it as quick as possible and with the lowest possible operative cost and failure risk.

At this point, all the solutions have founded an effective way to achieve the update.
Each solution will be more or less efficient and in some cases, manual tasks must be carried out.

The aim is that each anti-virus client be as autonomous as possible in terms of updates, so that each unit of the organization is updated as soon as it is turned on or the moment a new update is made available. If the unit is a portable one, or for some reason the management server is not available, even is that case the unit will be updated.

Annex 2 compares the characteristics of the different updating procedures, which may be implemented with each solution.

The analysis of this table, allows us to observe that all of them are permitting (with a greater or lesser difficulty, and with a higher or lower number of weak points) a periodic daily update at the least.

The architecture chosen by each organization, and the signature update policy at the workstations, together with the delay proper of a new signature, will indicate us how long will we be unprotected as against the attack of a new virus. Therefore, the probability of an infection will be increased directly in relation to its capacity to spread.

6) Analysis of the frequent propagation methods of some of the last viruses that appeared during the period May-June, 2003

How can a virus reach a PC in order to infect it?

Although these are not the only propagation methods, (as the analysis is confined to the propagation methods of the 15 viruses chosen) I will be able to recognize that the methods used by them particularly, would allow a quick spread in any network without a strong security policy implemented and kept seriously.

On the other hand, this analysis will give us the necessary guidelines which will then enable us to put forward security policies specifically for anti-virus software, as well as supplementary procedures in order to reduce the risk related to the time of response in connection with new viruses.

Annex 3 compares the different methods used by the chosen virus in order to spread through the Internet and through local networks.

The spreading through the Internet is primarily led by the traffic of mail attachments containing files executable with the virus, or links to infected sites, which could allow the spreading through the user's browser without his consent. In some cases, the virus may be a part of the body of the mail, trying to exploit some known vulnerability of the mail client for its execution without consent.

- It spreads via e-mail as an attachment with a certain extension (exe, com, vbs, scr, pif, bat, ocx, etc.)
- It spreads via e-mail as an attachment with a zip extension.
- It spreads through a link to a website that unloads and executes the virus.
- It exploits vulnerabilities of a browser or e-mail client and of the Operating System.

Once the first unit of a network is infected, the virus will attempt to spread within the LAN, and to any other unit that could be reached as from a local reference (e-mail address book).

Some virus, will attempt to spread through files exchange applications, or instant-messaging services, by using any active connection set.

Besides, it will modify the system in a manner convenient for it, so that it continues to exist after restarts or power cuts, and it will stop the services related to security applications (anti-virus software) which, should it be updated, would be able to detect them.

If it finds difficulties in order to spread through the e-mail client set at the workstation used by the unit, some of them have their own e-mail client embedded, and a list of servers that may be used in order to carry out this e-mails relay.

- It spreads through shared drives.
- It spreads through "port 135,139".
- It spreads through P2P File Sharing (KaZaA, etc)
- It uses a dictionary-style attack.
- Its forwards itself using an e-mail client defined in the system.
- It spreads via e-mail using its own SMTP engine.

Disinfecting an affected system is usually expensive in terms of the man-hours necessary for each infected unit, and of the hours in which the user in charge of the unit is not productive.

Each virus has its own cleaning procedure, none of which is “simple, quick and nice”, and usually, when a unit is infected, the rest of the units must be considered suspicious and this implies that the entire organization requires a revision.

On the other hand, from the user point of view, the “Infected and cured” unit is a unit which could not be considered reliable, and it is usual to find requirements for the reinstallation of the workstations related to units which do not work properly after being infected by a virus.

7) Recommendations on preventive measures that could be taken in an organization in order to reduce the risk of infection through new viruses

The three previous items attempted to show a portion of the scenario in which we are nowadays.

They are not very encouraging but explain the reason why we keep having problems despite having better Anti-virus software and better anti-virus security policies.

Now, we update anti-virus signatures every few hours, we protect e-mail, we have a greater control over the local settings of the anti-virus client for each workstation, we handle alerts in real time, and despite all that we may suffer a virus attack at any moment.

In some cases, we also protect traffic from the internet (HTTP, FTP) through anti-virus gateways solutions within the perimeter.

The truth is that after reading carefully about the methods used by the viruses in order to spread through the Internet and the local networks, we could decide to make their work a little bit more difficult.

The idea is that preventive measures, changes in the settings of some systems, and the reeducation of the users' habits may be carried out in order to reduce even more the probability of an infection by new viruses.

Let us see some points explaining previous annex 3.

It spreads via e-mail as an attachment with a certain extension (exe, com, vbs, scr, pif, bat, ocx, etc.)	✓ **The messaging services (e-mail servers) should be set again so that they do not allow the inbound and outbound of e-mails containing attachments with extensions traditionally used for the spreading of viruses** ✓ **Users should be reeducated in order for them to send their e-mail attachments compressed so that the creation of a temporary file be forced (during the process of decompression giving the anti-virus client the chance to scan a file which otherwise could be directly executed by the "Virtual Machine" of the e-mail client).** ✓ **Anti-Spam mail solutions should be implemented.** ✓ **Firewall policies should be implemented in order to not allow outgoing smtp traffic from any other than that from the internal mail server** ✓ **Workstations' settings should be reestablished so that they do not hide the extensions of known files (this would also avoid the spreading of attachments with double extension, which are usually accessed by the user directly from the mail client without saving it first on disk)**

It spreads through a link to a website that unloads and executes the virus.	✓ Anti-virus protection for the perimeter (http, ftp) should be provided for the detection of a malicious active code filtered by content (what kind of objects may enter the network and under which conditions) ✓ Internet access policies should be implemented, limiting access to websites not related to the organization's activity, or doubtful sites, in terms of the content, the user or unit, the time, etc. This solution is usually related to another problem, which is closer to the productivity of the users and the unauthorized use of systems, but which would be useful in order to avoid the spreading of viruses and last generation threats (ActiveX control and malicious Java App). ✓ Security patches should be applied in relation to the mail client and the Internet browser **(see Annex 5).**
It exploits vulnerabilities of a browser or e-mail client and of the Operating System.	✓ **Manager systems should be mended:** o **By removing non-corporate or unauthorized software.** o **By removing unnecessary services in both servers and workstations.** o **By applying services packs, patches and hotfix for operating systems and office applications (see Annex 5).** ✓ **The settings of the security levels for the Workstation and server browser should be redefined.**

It spreads through shared drives.	✓ **Shared drives should also be allowed in file servers.** ✓ **In the case, shared drives are required at workstations; safe settings should be established (minimum access privileges, limited access to certain users, access protected by means of passwords, read-only files, auditing of shared drives.)** ✓ **Strong password policies should be implemented.** ✓ **The workstations should be periodically audited in order to look for violations to this policy and immediate action should be taken aimed at its correction (this may be done using vulnerability scanner tools or share finders tools)**
It spreads through "port 135,139" (Administrative Shared drive C$)	✓ Strong password policies should be implemented (So as to avoid the success of the dictionary-style attack)
it spreads through P2P File Sharing (KaZaA, etc)	✓ **The installation of software by unauthorized personnel should be prohibited, and the minimum and safe settings to be implemented in each case should be checked.** ✓ **The implementation of non-corporate or personal software (instant messaging services, downloading managers, files managers) should be prohibited.** ✓ **Firewall policies should be applied in order not to allow the traffic of these applications.**
It uses dictionary-style attack	✓ Strong password policies should be implemented. ✓ The blocking of the account by wrong password should be enabled.

Its forwards itself using an e-mail client defined in the system	✓ Security patches should be applied to MS Outlook clients, in order to avoid that the APIs be called upon by applications other than those belonging to the same mail client. **(4)**
It spreads via e-mail using its own SMTP engine	✓ **Firewall settings limiting the incoming or outgoing smtp traffic should be established only in relation to the ip addresses of mail servers, and in this will not allow a virus to take infected e-mails out and the clients to use another non-corporate mail service (this does not avoid the use of webmail, which could be limited using a web Control solution).**

8) Conclusion

The anti-virus solutions, which are available nowadays, are highly effective, powerful and of long reach. The fact that all the organizations must have an anti-virus (either one of those which have been evaluated or any other that which better fits their needs) solution is unquestionable.

Shifting the responsibility for an infection to the solution vendor or to the user of the infected unit implies not to understand the problem that we are facing.

Vendors may improve their time of response, but they will always depend on a first reported incident to get the evidence. In order to generate the detection patterns as well as the cure, they react as against an incident and they run to avoid that said incident be repeated in relation to other clients.

Users act according to habits, customs and needs, and they may be educated in order to do their work bearing in mind security matters.

Any organization must be aware of the value of its assets, and of how important maintenance tasks are in relation to the critical mission systems and to the users' workstations for the continuity of the organization's activities. There is still a lot of work to be done in this area.

Those responsible for the security must be alert, so as to determine which habits, customs or needs are putting the organization's assets under risk of infection by virus, and which maintenance activities which are not being carried out (due to lack of time, personnel or budget) may also increase the risk of infection by virus over the assets. They must report it and help to correct it.

The preventive measures put forward in this paper, may help you avoid the spreading of a virus to your entire network or to save precious minutes during a massive infection. As well as the recommendations proponed are part of the minimum requirements of other Security policies, so if you are thinking of formalizing all security policies of your organization, it is important to take them into account, to consider them as part of an aggregate where policies are interrelated among them.

9) References

1) Market share of Corporate Antivirus solution

This is a proximal value for Latin America market share, this value is provided by these vendors in his local sales meeting.

2) Specific products and vendors references

Manuals of the assessed products:

CA:
http://support.ca.com/products/nt/inocit-manuals.html
Trend
http://www.trendmicro.com/download/product.asp?productid=17&show=doc
http://www.trendmicro.com/download/product.asp?productid=5&show=doc
Symantec:
http://www.symantec.com/techsupp/enterprise/products/sav_ce/sav_8_ce/manuals.html
Network Associates:
http://www.networkassociates.com/common/media/mcafeeb2b/support/VSE/VSE_70_ConfigGuide_ePO_25x_EN.pdf
http://www.networkassociates.com/common/media/mcafeeb2b/support/VSE/VSE_70_ProductGuide_EN.pdf
http://www.networkassociates.com/common/media/mcafeeb2b/support/VSE/VSE_70_InstallGuide_EN.pdf
http://www.networkassociates.com/common/media/mcafeeb2b/support/VSE/VSE_70_CONFIG_GUIDE_EPO_30_EN.pdf
http://www.networkassociates.com/common/media/mcafeeb2b/support/VSE/VSE_70_ImplementationGuide_EN.pdf

Signatures and engines updates

CA:
http://support.ca.com/Download/virussig.html
NAI:
http://www.nai.com/us/downloads/updates/default.asp
SYMATEC:
http://securityresponse.symantec.com/avcenter/download/pages/US-N95.html
TREND:
http://www.trendmicro.com/download/pattern.asp
http://www.trendmicro.com/download/engine.asp

List of the last virus detected and of on-line libraries

CA:
http://www3.ca.com/virusinfo/
NAI:
http://vil.nai.com/vil/newly-discovered-viruses.asp
SYMANTEC:
http://securityresponse.symantec.com/avcenter/vinfodb.html
TREND:
http://www.trendmicro.com/vinfo/

3) References on CSI/FBI

http://www.gocsi.com/forms/fbi/pdf.html (it requires the provision of data of the person requesting it for reading purposes, it is a document free of charge)

4) Microsoft security patches

Outlook Patch to oblige to save attachment files in disk
<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q235309&id=KB;EN-US;Q235309>

Other security patches for MS Outlook
<http://office.microsoft.com/downloads/2000/Out2ksec.aspx>
<http://office.microsoft.com/downloads/9798/Out98sec.aspx>

Microsoft: Patch Management, Security Updates, and Downloads

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/patch/default.asp>

Annex 1

Comparative chart of the issue of signature update per each assessed virus.

Date of Virus Signature Update

Virus Name				First signature	SYM (LU)	NAI	CA	TREND	Wild/reported Infection	Destructiveness/ damage potencial	Pervasiveness/ distribution potencial	General
	REF											
worm	12	SYM	W32.HLLW.Fizzer@mm	5/9/2003	0	3	3	3	high	medium	high	x
		NAI	W32/Fizzer@MM						x	x	x	medium
		CA	Win32.Fizzer						medium	medium	medium	x
		TREND	WORM_FIZZER.A						medium	high	high	medium
worm	1	SYM	W32.Femot.Worm	6/4/2003	0	7	2	1	medium	medium	medium	x
		NAI	W32/MoFei.worm						x	x	x	low
		CA	Win32.Mofei.A						low	medium	medium	x
		TREND	WORM_MOFEI.A						low	high	medium	low
worm	2	SYM	W32.Bugbear.B@mm	6/4/2003	1	1	1	0	high	medium	high	x
		NAI	W32/Bugbear.b@MM						x	x	x	medium
		CA	Win32.Bugbear.B						high	medium	high	x
		TREND	PE_BUGBEAR.B						low	high	high	low
worm	3	SYM	W32.Mapson.Worm	6/7/2003	0	4	3	2	medium	low	high	x
		NAI	W32/Mapson@MM						x	x	x	low
		CA	Win32.Mapson.A						low	low	high	x
		TREND	WORM_MAPSON.A						low	high	high	low
worm	8	SYM	W32.Redzed@mm	6/11/2003	0	14	0	10	low	medium	high	x
		NAI	W32/Gant.d@MM						x	x	x	low
		CA	Win32.Thaprog.C						x	x	x	x
		TREND	WORM_GANT.C						low	high	high	low
worm	15	SYM	W32.Naco.D@mm	6/12/2003	6	0	1	0	low	high	high	x
		NAI	W32/Naco.f@MM						x	x	x	low
		CA	Win32.Naco.E						low	medium	high	x
		TREND	PE_NACO.F						low	high	high	low
worm	14	SYM	W32.Danvee@mm	6/18/2003	0	0	5	1	low	low	high	x
		NAI	W32/Danvee@MM						x	x	x	low
		CA	Win32.Crock.A worm						x	x	x	x
		TREND	WORM_CROCK.A						low	high	high	low
worm	5	SYM	W32.Sobig.D@mm	6/18/2003	0	3	0	1	low	low	high	x
		NAI	W32/Sobig.d@MM						x	x	x	
		CA	Win32.Sobig.D						low	medium	high	x
		TREND	WORM_SOBIG.D						low	high	high	
worm	10	SYM	W32.Randex.C	6/19/2003	0	0	5	3	low	medium	medium	x
		NAI	W32/Randex.c						x	x	x	low
		CA	Win32.Mongue.A						low	medium	slow	x
		TREND	BKDR_RANDEX.C						low	high	low	low
trojan	13	SYM	Trojan.Systrim	6/19/2003	13	6	3	0	low	medium	low	x
		NAI	Sniff-Systrim						x	x	x	Low-Profiled
		CA	Win32.Systrim.A						low	medium	Not Distribute	x
		TREND	TROJ_SYSTRIM.A						low	high	low	low
trojan	9	SYM	Trojan.Linux.Typot	6/21/2003	4	4	1	0	low	low	low	x
		NAI	Linux/Typot						x	x	x	low
		CA	Linux/Typot.A						low	low	Not Distribute	x
		TREND	ELF_TYPOT.A						low	medium	low	low
worm	6	SYM	W32.Sobig.E@mm	6/25/2003	0	0	0	1	high	medium	high	x
		NAI	W32/Sobig.e@MM						x	x	x	
		CA	Win32.Sobig.E						medium	low	high	x
		TREND	WORM_SOBIG.E						low	high	high	
worm	4	SYM	W32.Mumu.B.Worm	6/26/2003	0	4	1	0	medium	medium	medium	x
		NAI	W32/Mumu.b.worm						x	x	x	low
		CA	Win32.Mumu.B						high	medium	high	x
		TREND	WORM_MUMU.B						low	high	high	medium
worm	7	SYM	W32.Vivael@mm	6/28/2003	0	2	2	3	low	low	high	x
		NAI	W32/Colevo@MM						x	x	x	Low-Profiled
		CA	Win32.Colevo						low	low	high	x
		TREND	WORM_COLEVO.A						low	high	high	low
worm	11	SYM	W32.Klexe.Worm	6/28/2003	0	2	1	3	low	low	high	x
		NAI	W32/Klexe@MM						x	x	x	low
		CA	Win32.Klexe.A						low	low	medium	x
		TREND	WORM_KLEXE.A						low	high	high	low
		Average			**1.60**	**3.33**	**1.87**	**1.87**				

Annex 2

Comparative chart of signature updating procedures

		Computer Associates	Network Associates	Trend Micro			Symantec	
	Firsts machine that update his signature and its firm and puts it to disposition of the remainder.	Redistribution server (any client or the Admin Server)	ePolicy Orchestrator	TMCM: ServerProtect - OfficeScan	ServerProtect	OfficeScan (server or client)	Live Update	Intelligent Update
	Download protocol	ftp	ftp/http	http/ftp	http/ftp	http/ftp	ftp	http
	Owner of the sources	proprietary	outsorcing	outsourcing	outsourcing	outsourcing	proprietary	proprietary
	Provider		akamai	akamai	akamai	akamai		
1° Tier	Type of download	pull	pull	pull	pull	pull	pull	pull
	Automatic	Yes	Yes	Yes	Yes	Yes	Yes	No
	Manual	Yes	Yes	Yes	Yes	Yes	No	Yes
	minimum frequency allowed	minute	minute	hour	hour	hour	daily	N/A
	Fequency stándar of new updates (guaranty for the vendor)	daily	daily	daily	daily	daily	weekly	daily
	More frequency are contemplate	2 or 3	2 or 3	2 or 3	2 or 3	2 or 3	2 or 3	2 or 3
	Incremental Update	Yes	Yes	Yes	Yes	Yes	Yes	No
	The engine update (If is necessary) are a separate Process ?	No	No	Yes	Yes	Yes	No	No
2° Tier	Client update	clients	clients	Servers-clients	others servers	clients	clients	clients
	At startup	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	On demand	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Automatic	No	Yes	Yes	Yes	Yes	Yes	Yes
	Scheduled	Yes	Yes	Yes	Yes	Yes	Yes	No
	From server	Yes	Yes	Yes	Yes	Yes	No	Yes
	Type	pull	pull	pull	pull	pull	pull	push
	Frequency	minute	minute	daily/minute	hour	minute	daily	N/A
	FTP	Yes	Yes	No	No	No	Yes	No
	HTTP	No	Yes	Yes	Yes	Yes	Yes	No
	Share / UNC	Yes	Yes	Yes	Yes	No	Yes	No
	Local path	Yes	Yes	No	Yes	Yes	No	No
	Allow distributed Update sources	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Allow multiple sources of update	Yes	Yes	Yes	No	Yes	Yes * (some platform)	No

Annex 3

Comparative chart of the propagation methods of each assessed virus.

	it spreads via e-mail as an attachment with a certain extension (exe, com, vbs, scr, pif, bat, ocx, etc.)	it spreads via e-mail as an attachment with a zip extension.	It spreads through a link to a website that unloads and executes the virus.	It exploits vulnerabilities of a browser or e-mail client and of the Operating System.	it spreads through shared drives.	it spreads through "port 135,139"	it spreads through P2P File Sharing (KaZaA, etc)	it uses a dictionary-style attack.	its forwards itself using an e-mail client defined in the system.	it spreads via e-mail using its own SMTP engine.
virus #										
1					Yes	Yes		Yes		
2	Yes			Yes	Yes				Yes	Yes
3	Yes						Yes		Yes	
4				Yes	Yes	Yes		Yes		Yes
5	Yes				Yes					Yes
6		Yes			Yes					Yes
7	Yes									Yes
8	Yes						Yes		Yes	
9	Trojan									
10				Yes	Yes	Yes		Yes		
11		Yes	Yes						Yes	
12	Yes						Yes		Yes	Yes
13	Trojan									
14	Yes								Yes	
15	Yes				Yes		Yes		Yes	

Annex 4
Report for each assessed virus.

Virus #	Vendor	Virus Name	URL of virus description
1	SYM	W32.Femot.Worm	http://securityresponse.symantec.com/avcenter/venc/data/w32.femot.worm.html
	NAI	W32/MoFei.worm	http://vil.nai.com/vil/content/v_100357.htm
	CA	Win32.Mofei.A	http://www3.ca.com/virusinfo/virus.aspx?ID=35505
	CA	Win32.Mofei.A	ftp://ftp.ca.com/pub/InocuLAN/4342add.txt
	TREND	WORM_MOFEI.A	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MOFEI.A
2	SYM	W32.Bugbear.B@mm	http://securityresponse.symantec.com/avcenter/venc/data/w32.bugbear.b@mm.html
	NAI	W32/Bugbear.b@MM	http://vil.nai.com/vil/content/v_100358.htm
	CA	Win32.Bugbear.B	http://www3.ca.com/virusinfo/virus.aspx?ID=35384
	TREND	PE_BUGBEAR.B	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=PE_BUGBEAR.B
3	SYM	W32.Mapson.Worm	http://securityresponse.symantec.com/avcenter/venc/data/w32.mapson.worm.html
	NAI	W32/Mapson@MM	http://vil.nai.com/vil/content/v_100364.htm
	CA	Win32.Mapson.A	http://www3.ca.com/virusinfo/virus.aspx?ID=35466
	TREND	WORM_MAPSON.A	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MAPSON.A
4	SYM	W32.Mumu.B.Worm	http://securityresponse.symantec.com/avcenter/venc/data/w32.mumu.b.worm.html
	NAI	W32/Mumu.b.worm	http://vil.nai.com/vil/content/v_100438.htm
	CA	Win32.Mumu.B	http://www3.ca.com/virusinfo/virus.aspx?ID=35656
	TREND	WORM_MUMU.B	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MUMU.B
5	SYM	W32.Sobig.D@mm	http://securityresponse.symantec.com/avcenter/venc/data/w32.sobig.d@mm.html
	NAI	W32/Sobig.d@MM	http://vil.nai.com/vil/content/v_100397.htm
	CA	Win32.Sobig.D	http://www3.ca.com/virusinfo/virus.aspx?ID=35549
	TREND	WORM_SOBIG.D	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SOBIG.D
6	SYM	W32.Sobig.E@mm	http://securityresponse.symantec.com/avcenter/venc/data/w32.sobig.e@mm.html
	NAI	W32/Sobig.e@MM	http://vil.nai.com/vil/content/v_100429.htm
	CA	Win32.Sobig.E	http://www3.ca.com/virusinfo/virus.aspx?ID=35652
	TREND	WORM_SOBIG.E	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SOBIG.E
7	SYM	W32.Vivael@mm	http://securityresponse.symantec.com/avcenter/venc/data/w32.vivael@mm.html
	NAI	W32/Colevo@MM	http://vil.nai.com/vil/content/v_100450.htm
	CA	Win32.Colevo	http://www3.ca.com/virusinfo/virus.aspx?ID=35704
	TREND	WORM_COLEVO.A	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_COLEVO.A
8	SYM	W32.Redzed@mm	http://securityresponse.symantec.com/avcenter/venc/data/w32.redzed@mm.html
	NAI	W32/Gant.d@MM	http://vil.nai.com/vil/content/v_100409.htm
	CA	Win32.Thaprog.C	ftp://ftp.ca.com/pub/InocuLAN/4347add.txt
	TREND	WORM_GANT.C	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_GANT.C
9	SYM	Trojan.Linux.Typot	http://securityresponse.symantec.com/avcenter/venc/data/trojan.linux.typot.html
	NAI	Linux/Typot	http://vil.nai.com/vil/content/v_100406.htm
	CA	Linux/Typot.A	http://www3.ca.com/virusinfo/virus.aspx?ID=35608
	TREND	ELF_TYPOT.A	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=ELF_TYPOT.A
10	SYM	W32.Randex.C	http://securityresponse.symantec.com/avcenter/venc/data/w32.randex.c.html
	NAI	W32/Randex.c	http://vil.nai.com/vil/content/v_100401.htm
	CA	Win32.Monque.A	http://www3.ca.com/virusinfo/virus.aspx?ID=35631
	TREND	BKDR_RANDEX.C	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=BKDR_RANDEX.C
11	SYM	W32.Klexe.Worm	http://securityresponse.symantec.com/avcenter/venc/data/w32.klexe.worm.html
	NAI	W32/Klexe@MM	http://vil.nai.com/vil/content/v_100449.htm
	CA	Win32.Klexe.A	http://www3.ca.com/virusinfo/virus.aspx?ID=35687
	TREND	WORM_KLEXE.A	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_KLEXE.A
12	SYM	W32.HLLW.Fizzer@mm	http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.fizzer@mm.html
	NAI	W32/Fizzer@MM	http://vil.nai.com/vil/content/v_100295.htm
	CA	Win32.Fizzer	http://www3.ca.com/virusinfo/virus.aspx?ID=35131
	TREND	WORM_FIZZER.A	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_FIZZER.A
13	SYM	Trojan.Systrim	http://securityresponse.symantec.com/avcenter/venc/data/trojan.systrim.html
	NAI	Sniff-Systrim	http://vil.nai.com/vil/content/v_100398.htm
	CA	Win32.Systrim.A	http://www3.ca.com/virusinfo/virus.aspx?ID=35607
	TREND	TROJ_SYSTRIM.A	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_SYSTRIM.A
14	SYM	W32.Danvee@mm	http://securityresponse.symantec.com/avcenter/venc/data/w32.danvee@mm.html
	NAI	W32/Danvee@MM	http://vil.nai.com/vil/content/v_100380.htm
	CA	Win32.Crock.A worm	ftp://ftp.ca.com/pub/InocuLAN/4357add.txt
	TREND	WORM_CROCK.A	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_CROCK.A
15	SYM	W32.Naco.D@mm	http://securityresponse.symantec.com/avcenter/venc/data/w32.naco.d@mm.html
	NAI	W32/Naco.f@MM	http://vil.nai.com/vil/content/v_100331.htm
	CA	Win32.Naco.E	http://www3.ca.com/virusinfo/virus.aspx?ID=35473
	TREND	PE_NACO.F	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=PE_NACO.F

Annex 5

Automatic deploy of fixes (software delivery solutions).

Commercial products

- IBM Tivoli
- CA Unicenter Software Delivery
- Novell ZENwork
- Microsoft SMS

Free solution:

- KixStart,

KixStart can be used in any windows platforms.

"The KiXtart (Kix32.exe) tool included on the Windows NT Server Resource Kit version 4.0 CD-ROM (this tools is not supported by Microsoft Product Support Services provides some networking functionality for Windows NT that is not built-in to the Windows NT user interface. KiXtart is a login script processor and enhanced batch language for Windows NT"
(http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b175732)

"The KiXtart free-format scripting language can be used to display information, set environment variables, start programs, connect to network drives, read or edit the registry change the current drive and directory and much more.
KiXtart 2001 was developed by Ruud van Velsen of Microsoft Netherlands"
(http://www.kixtart.org/)