Halmstad University
Network Security

Anti-virus Techniques

Authors
Boris Bruse
Stefan Björk-Olsén
Martin Hafstrand

2008-05-13

CONTENTS

Sources for all writers can be found on page 14 and forward.

Introduction

Before the age off computers and server come the most useful thing was then to use off typewriter and then collect that information in maps and catalogs on the company or at in home. If somebody wants to see or have use off your material you send with post or perhaps fax over to that person.

When computer get in the era first in business and then at home ,you could do the same thing but more fare faster ,you could off course also here save your work in maps and catalogs. To understand the forthcoming struggle that will come in our way with or the other side off the coin ,we first must se and have a short understanding off who a computer works .

A computer is rather dumb, in that way is only thing its matter is one and zero nothing more nothing less, in another way on and off. The main operative system tells what to do, when to do them and under which circumstances. In the operation system are also the file system, If I want to write a letter the commands and instructions for that specific task is given the computer and do what its told, no question asked if off course not sort off misbehavior instruction. Because in the beginning virus and other sort off malware was rather uncommon and an antivirus protection application was not built in the OS or an extra layer application the trick to lure the file system was not especially hard.

The first virus for computer come across 1986 that virus was a simple boot virus MS dos ,its function is to interrupt the boot startup process it was not a potentially "bad " virus in a definition in why ? because its spreading with the most common way in those days .With a floppy disk 1.44 mb if the floppy was still insert in the computer and the computer start up then the boot sector was to be infected The internet infrastructure was in the early rising so its was not a big threat. [1] The ordinary way to infect a host was simple to change the input from example your letter.txt to your letter.exe .A big success in this way was because windows on default not check the ALL file extension length ,in that way the ending could be example .exe instead for .txt Before wee go further in this virus analyst and behavior technique we most now what is the different between worms and virus ?

The big different are at that a virus are spreading INSIDE a computer and damage the environment in one or another way most way to get a virus is by example by e-mail and I DO something I OPEN the e-mail. A worm is spreading OUTSIDE a computer by the ETHERNET and also do NOT need an ACTION example some sending a mail .its spreading itself and in a very rapid way off course. [2]. the clear goal for a malicious antivirus maker is to make a virus 1.invissible,undetecteball. In that way the use all off the legal opportunity that’s stand by in the computer world ,which means .1.zip files.2.use off encrytion.3poliformic behavior.

Today at 2008 and forward antivirus problem it’s raising because its main sources it’s not any longer the ,script caddie or ,pure hacking sabotage. Today a sort off new era is coming with cyber organization criminals how goals are to 1. Get information, from company or privacy person to get money, critical information or disturb infrastructure.

Anti-virus programs

A question raises ,are viruses ding out or are the limit in ? The answer is not.
Quote from **Panda labs**. " **Even though some security experts out there maintain that '*viruses are a thing of the past*', the fact is that almost 20% of the new malaria we see every month are self-replicating viruses and worms. This figure is not as high as it used to be years ago but it comes to prove that viruses are definitely not dead. " end off quote [5]**

So what techniques are used in antivirus solution ?
There are two ways there techniques use. The first one is so at say a white/blacklist off known codes or protocols that the antivirus engine scan against. When new viruses arrives the user get an update from the antivirus company database the time the gets update differ from antivirus-company, but today its now flexing from our to in a week span.

But who should we handle the time between updates and unknown viruses? If you get an update so at say every tree days ,lots off things can happen in that time span.
So what is the solution?
Its calling behavior analysis which means at the antivirus engine now when its se that there is no known code or white/blacklist its analyses the behavior off WHAT that specifically file DO, what processes are called? How much system resources are in use?

The third way is to have a protected environment behind the computer software and the new known files or program coming down to the computer. In that case its a way to use "sandbox" ordinary wee thinking off a playground for children and its not at all a bad example its better there dig and digging around there and in your rose garden . Same here to have a virtual sandbox who like and pretend to be the "original" computer system the antivirus engine can lure out the bad behavior from the bad files /program and do no harm against the original operation system .[6]

So how stand the competition against the different antivirus techniques and manufacturers ?

They basically all work today with in principal in mind.

Bitdefender.[7]Use first the standards way off signature based check. But the also use the so called "sandbox" model. Which exactly means that the antivirus engine analyses for behavior and bad files/program in a protected virtual environment. They called that for B-HAVE

MacAfee.[8] Have two interfaces to source 1.Realtime 2.Manual. In the real-time scan the uses the heuristic technique to search for known viruses and new variants off new viruses.

Avast.[9] Have in version 4.8 first the ordinary signature file scan type. And then there the also have GMER. What is that ? [10] its a application who among lot off things analyses also check for root kits.

Nod 32.[11]Have also the ordinary signature scan ,but also the proactive method they called ThreatSense technique. What is that? That is a all in one solution which means signature analysis AND proactive analysis in the same engine.[12]

Panda security.[13] Panda its going its own way in that since there are NO certification for their products.
The analysis method they have is the ordinary known list then they also have a technique they called Trueprevent[14] and that is a behavior analysis for known viruses. They also have a huge community database off samples off known viruses called 'nano' scan [15]which if you have there's product you can also get virus and other malware taken care off.

Kaspersky[16]Antivirus have so at say three in one technique the first is to update the database off signature on a hourly time. The two next is proactive behavior analysis. Kaspersky also have protection for cell phones.

F-secure.[17]Antivirus has standard analysis and also a method who they called .F secure Deep Guard technology.
How is a proactive behavior analysis method. F-secure also have protection for cell phones.
Norman[18] Norman antivirus. They have a flagship which they call 'unique sandbox model off behavior analysis'[19]

Norton Symantec.[20] has the ordinary signature method. Then they have a method they called , SONAR, its behavior analytics.

A good choise is to check with a neutral certifier company like Icsalabs. (https://www.icsalabs.com/icsa/main.php?pid=b31a$6140dfe3-4a851ebd$eaa4-72b) or Av Comparatives. (http://www.av-comparatives.org/).

Especially this link it's interesting because its show an hint off what the struggle in capture hardened viruses is a never ending work and also a balance between user-friendly (fast scan) and high detection rate.
http://www.av-comparatives.org/seiten/ergebnisse/report17.pdf

In this analysis its clear that all off the antivirus companies are to go further with the proactive ,behavior analyze method off course with companionship with the ordinary database signature files list.
They all make really good effort to us the user to be safer on the net and protect the environment. One point you must include in this scenario is ,that matter nothing at all if you have a very god antivirus solution so what ever ,IF that can bypassed. And for certain it's the first they try and matter a thief or burglar does its a little bit off common since. I took up this because today most antivirus solution is ALL in ONE which means that firewall, antirootkit, adware and virus protection are built in. If it's bypassed in that way that you THINK you have protection its is really bad.

To see and get a hint off which ones all included antivirus and firewall companies who have not manage that you cold look at matousec transparent security [21]

THE FUTURE

So to the big question who look the future out for the companies who try do better antivirus protection ,and for the end user interface. Ipv6[22] it's now rolling out it's a great shift from a security point with IPSec.
Another rather important in security is implementation off DNSSEC which short describes is a authentication function with public key and encryption. The essence off this DNSSEC is to in secure way verify that domain A is really that domain I get response from and not a redirected domain.[23]

Beyond that the future seems a constant struggle against the antivirus problem with "new" growing internet countries with more inexperienced user and more and more off the IT infrastructure are coming to depend on the web and network, the battle against this only problem is not going to solve itself in a near future.

Intro

This part of the paper contains information about virus detection, viruses that avoid detection, repair or delete infected files and prevention. There is also a short notice about new platforms for viruses, under the 'IM and Community viruses' section.

One last thing that will be covered later on in this paper, under the section "Future" is that many people claim that signature based anti virus detection is getting outdated and are a thing of the past.

Detection

A virus signature, also called definition/DAT file, is either a hash or an algorithm that identifies a specific virus. In the hash case it is simply a hash of a part of code specific to the virus that signature is made for and the algorithm may for example look for certain behavior in a file and when it detects these certain actions it often flags the file and reports to the user.

Signatures are often made so that the code in question will probably be present in similar viruses, often referred to as being from the same 'family'. This makes the antivirus not only efficient against the known viruses but also to new forms of those viruses. This is called 'Generic detection'. Algorithm or "heuristic analysis" looks for odd behavior in files and programs to detect new viruses and new versions of previously known viruses.

When a new virus is discovered and is not fully or partially covered by other signatures a new one has to be created by the Antivirus company and then distributed out to the users. A problem with this is time, not only does the signature creation take time but the distribution make also take it's fair share of time due to the fact that some companies only updates the signatures once a week unless it is considered absolutely critical.

Another problem may be poorly designed signatures that may detect viruses where they are none due to the same coding in both the virus and the file or program in question. This is often referred to as a "False Positive"

Avoid Detection

An anti virus may use several ways to mask it's presence from the Anti-Virus programs. The four more common ones are Cavity, Disable Anti-virus, Polymorphic and Metamorphic. The two later are more covered in Martin Hafstrands report and will not be presented here but the two first will be

-Cavity virus

This virus is of such a small size so that it can place itself in unused areas of an exe file and by that not change or damage the exe file. There is a known virus, named CIH (A.k.a. Chernobyl or Spacefiller) that were active in the late 90's/beginning of 2000. It is considered one of the most harmful viruses around because it corrupted data on the hard drive and even in some cases even corrupted the BIOS, making the computer not able to boot.

-Disable Anti-virus

The other way of avoid detection is to go for the source of the 'problem' – the anti virus program. This can be done in multiple ways, either just disabling the Anti-Virus program from the startup sequence of the operating system, remove the specific signatures from the anti-virus programs signature database or even telling the anti-virus to exclude certain, those infected by the virus, files from the search. Most of these ways are now outdated and are corrected by either CRC-checks on the AV's signature database or having the operating system to monitor that the anti-virus is running properly.

Repair

An anti-virus program basically has three ways of dealing with an infected file and also a special case. The first way to deal with an infected file is simple, just remove the virus part of the infected file and hope that the virus didn't write over anything. If the virus has the information is probably unretreivable. Next way to deal with a file is to "quarantine" it, making it inaccessible by other programs and preventing it from running. This is done either if the file is undeletable or you need by some reason to save the infected file, either for research or because the data is irreplaceable and you hope finding a way to disinfect the file later. The third and last normal way an antivirus deals with an infected file is to simply remove the file altogether from the system. Usually when the other two methods prove not working or the file only consists of the virus. This method almost always works but sometimes not even normal deletion works. The file may for example claim to be a system file and therefore not removable, then most Anti-Virus problems deals with that by booting the anti-virus before you load you operating system and remove it there.

Then there all always really nasty viruses that hides outside the used space of a hard drive, in the boot sectors and even in the bios. But that kind of horror stories are better saved for another report.

Future

-Signatures are old.

There is a competition hosted on this years DefCon conversion called "Race to Zero" where the contestants are to modify a given set of virus and malicious code so that it passes through a rigorous set of antivirus. DefCon states that this in not aimed to create new viruses that fools anti-virus programs but rather to be entertaining for the participants. One common thought is that they are trying to make, not only the anti-virus companies, but also the consumers aware of that anti-virus signatures are a thing of the past. Many people feel that virus-signatures are a thing of the past and states things like "*I want to get off of signature-based antivirus as rapidly as possible. I think it's a broken model and I think it's an incredible CPU hog* " [1]

IM and Community viruses

Instant messaging and communities are growing larger every day and this is not going unnoticed by the virus creators.

Instant messaging application like Msn Messenger/Msn Live works like a new platform for distributing viruses. One common virus is a zipped file sent along with a message like “Hey, you got to check this pictures!”, once you open up the zip it contains malicious coding, usually in exe and when the user clicks it the virus, without the user knowing sends a copy of the zip file together with the same message to all your contacts in the users contact list. In that zip file any virus, worm or spy ware may be sent along, that to without the user’s knowledge.

Communities like My Space and Facebook are also targeted by viruses. One thing that might attract the virus creators may be the often extensive programming possibilities available on those sites where you can create your own plug-ins and add-ons. One example of that is a script that a person placed in his signature and everyone loading a page with his signature automatically ran that script and by that adding the creator to his or hers friends list and also adding that malicious script to their own signature. So the guy ends up with a million friends or so before the company closes his account. No real harm done but this may very well be used to distribute more harmful codes, like deleting the users profile, launching unwanted pages and downloading harmful software.

Martin Hafstrand – Viruses

A virus is itself a program which tries to do harm, it do so by copying itself to other files. .exe are what we use today to execute programs as in a windows systems which are what the virus needs since it want to remain hidden. If a virus executes itself as a program then it would be easily detected while doing whatever harm it's instructed to do. That's why a virus copy itself to other executable files which in turn slightly modifies what may be a commonly used program.

The new file does the same thing, a virus might just make a copy of itself but at the same time it might even delete files. If you have huge data archives then it's always important to make sure of having a virus free environment, a single virus could in worst case infect whole archives or delete, sabotage data which can be expensive and very important.

However these viruses that self replicates themselves and mainly just aim for destruction or to mess with people, which have become much smaller today. Some believe that by the more advanced and worst virus they make will give them a good reputation. Even small kids can create virus, so the highest amount of virus were made by people who just aimed to destroy things and didn't hide it. This was very easy to discover, however a new virus could just have had a different signature or been slightly changed to hide it presence. Hence this is why a bloodhound process was created which could figure what "might" have been a virus.

Anyone that stays updated or read new can notice that viruses isn't like they used to be and there's no big titles about dangerous viruses and those time that it were then it isn't that much to compare. The amount of viruses have become smaller but in turn much harder to detect, there may be a lot more virus lying and waiting out there but the detected rate is much less than it used to be

This was quite easy to catch since the virus aimed for destruction and in worst case a virus were detected right before any larger harm was done. However the last years there have been less viruses activity than it were before, now days it isn't small kids who make the viruses, it's professionals who don't plan to show off and describe what they did in a virus. Today people earn money on making virus by hiding and making viruses to a legal program, the Anti-virus sees this as a normal activity and doesn't concern itself about the file. When the virus is successfully spread out all over the system then the hacker might demand a big deal of money were he in the other case would erase archives and even more expensive data.

However even if the time have changed then there'll always be a huge virus which aims for just cause as much damage as possible, one of these were W32.Blaster.Worm. The virus was placed in the worm category and but do still function like a virus, in many cases or mostly you don't send a pure virus and how you define them is different. As mention earlier, a virus act inside a computer, but it cannot spread to the outside by itself so it's combined with a worm, in many cases a Trojan are used to open a path for the worm to enter and then the virus will act.

"*They can also affect other systems in a multitude of ways. Both worms and Trojans, however, can "drop" viruses into systems.***"** Nearly everything is categorized as worms or viruses since the most effective way to do damage it to combine every element.

There are four main phases that a virus normally can be found in:

Dormant – The state where the virus will remain idle until it trigger by a function like a certain time.
Propogation – This state is were the virus begin to propagate and begin to spread over ones system, as mention it copy itself to file a it can be activated in like .exe. No harm is done yet however it'll continue to spread and if the virus develop itself then it'll be even harder to catch. Blaster exploited DCOM RPC services which was known as "Interface Buffer Overrun Vulnerability (BID 8205)".
Triggering – This is the activation state, like a switch. Blaster itself was discovered at August 11 in the year 2003, if the date were after 15th August then the virus were to put in an execution state. This lasted until 31st December and were repeated the 15th every month.
Execution – The script that Blaster had were to initiate a dos attack against Windowsupdate.com, if unavailable to attack the DNS then it would use the broadcast 255.255.255.255. A virus often kills one of the Svchost.exe services which will then force the computer to reboot if the right one is hit. You might then notice your screen going blue also knows as blue screen.

"The following strings are visible in the worm's code:
msblast.exe
I just want to say LOVE YOU SAN!!
billy gates why do you make this possible ? Stop making money and fix your software!!
windowsupdate.com
start %s
tftp -i %s GET %s
%d.%d.%d.%d
%i.%i.%i.%i
BILLY
windows auto update
SOFTWARE\Microsoft\Windows\CurrentVersion\Run"

Here we can see the file name Msblast.exe and in the near end it's supposed to create a file

Called "Billy", this were a mutex or mutual exclusion which made sure that only one instance of the program did run once activated. Blaster did as well add a registry key to make sure that Msblast.exe was launched every time windows boots up.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windows auto update = msblast.exe

This Virus did in the end made a damage over 2-10 billion dollars and it's said that many hundreds of thousands computers were infected, not to mention that the dollar was quite high during that time.

The virus itself does at most fit in the category of **Boot sector** from my view, the virus infects a master boot record (MBR) and then boots where the virus would be contained. Blaster booted and gave a blue screen, so it wasn't a virus which did the work while being in Windows user mode.

Other categories of viruses are:

Parasitic – The most common type of virus which copies itself and attach to other executable files.
Memory-resident – Reside or stays in the memory where it infect all other running programs, this can be easily detected but hard to prevent unless you got good instructions.
Stealth virus – The virus we see today, a lot of professionals use stealth viruses to hide and avoid antivirus systems.
Polymorphic – This type mutates and change it's signature after every infection, this is then hard to detect and a lot of new virus are older Poly- or Metamorphic that still remains and spreads. This works since many scans follow signatures and is why you made scans like bloodhounds which check for suspicious codes. A way that you hide them is often at system dates, keystroke combinations and encryption which makes it hard to detect what really were a virus.
Metamorphic – This may probably be concluded as the worst kind you can meet, add the statements above then every time it repeats the coping process it rewrites itself.

Appearance and behaviour changes as well and as instructed it do more or less create a whole new virus which might be completely different.

Mobile Devices

Something new that has grown quite much lately are virus for mobile platforms, why you target these systems is because there are more vulnerable against memory or processor demanding attacks. Meaning that would be very easy to easily flood the system or filling the hard drive, so a mobile device may get really slow or might in the end damage the system. Mobile systems are much harder to repair as well, and it's even harder if the device got a very low memory available to work with. About 400 mobile viruses exist today and it won't become less either, a virus is often downloaded by the user or by accessing a bad site which might have a hidden script. A virus can in the range steal your personal information to shut down your mobile device so it never works again, everything is possible.

Sources and references for Boris Bruse

[1] **Computer Knowlegde**
Author. Robert Slade: Chapter 7 - (c) Brain.
Last Changed: Tuesday, January 31, 2006
http://www.cknow.com/vtutor/RobertSladeChapter7-Brain.html

[2] **Symantec**
Author. Symantec AntiVirus Research Center
http://www.symantec.com/avcenter/reference/worm.vs.virus.pdf

[5] **Panda Reserch Blog**
leading the way in proactiv malware detection
Author. Pedro Bustamente edit at 09 May 08
Headline. New Malware Prevalence April 2008
Second rubrik. New Self-Replication Virus & Worms
http://research.pandasecurity.com/archive/New-Malware-Prevalence-April-2008.aspx

[6] **Viruslist.com**
Headline :Proactive Protection: a Panacea for Viruses ?
Author.Olig Gudilin. Senior Marketing Researcher of strategic marketing, Kaspersky Lab
edit at 28 Jun 2006
http://www.viruslist.com/en/analysis?pubid=189801874

Antiviruscompany

[7] **Bit defender antivirus 2008**
Advance proactive protection from viruses,spyware and more..
http://www.bitdefender.com/PRODUCT-2194-en--BitDefender- Antivirus-2008.html#more_features then go to Data Sheet
http://www.bitdefender.com/files/Main/file/datasheet_web-AV-2008-EN.pdf

[8] **Mcaffe**
Link to the product guides. http://us.mcafee.com/root/support.asp?id=retail_userGuides
http://download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf
Product manual in McAfee Internet Security user guide. chapter 10 ”setting up virusprotection”side 37.and side 38 ”setting real-time scan options”.

[9] **Avast**
http://www.avast.com/eng/avast-free-home-antivirus-antispyware.html#1

[10] **GMER**
http://www.gmer.net/index.php

[11] **ESET**
Antivirus Protection with ESET NOD32 and then follow the link .TreatSence technology:
http://www.eset.com/products/nod32.php

[12]Under products. Zero-Day Attack - Heuristics and Signatures software from ESET
http://www.eset.com/products/threatsense.php

[13] TruPrevent
http://research.pandasecurity.com/archive/How-TruPrevent-Works-_2800_I_2900_.aspx

[14] **Panda true prevent**
http://www.pandasecurity.com/homeusers/solutions/truprevent/truprevent-3.htm?sitepanda=particulares

[15] **Activ scan or nanoscan Panda**
http://www.pandasecurity.com/activescan/index/?track=1&Lang=en-US&IdPais=63
http://www.pandasecurity.com/infected_or_not/se/

[16] **Kaspersky Antivirus**
http://www.kaspersky.com/kaspersky_anti-virus

[17] **F-secure Antivirus**
http://www.f-secure.se/home_user/antivirus.html and under read more pdf
http://www.f- secure.se/export/system/fsgalleries/datasheets/fsav2008.pdf

[18] **Norman antivirus**
http://www.norman.com/Product/Home_Home_office/NVC/49922/

[19] **Norman pdf sandboxtecnice**
http://www.norman.com/Partner/Product_sheets/15885/se
http://www.norman.com/Product/ProductSheets/Norman_SandBox_eng.pdf/se

[20] **Norton antivirus**
http://www.symantec.com/about/news/release/article.jsp?prid=20070117_01

[21] **Matousec transparen security**
http://www.matousec.com/projects/firewall-challenge/results.php

[22] **IPv6 protocol**
http://www.ietf.org/rfc/rfc2460.txt

[23] **DNSSEC : RFC 4034**
http://www.rfc-archive.org/getrfc.php?rfc=4034

DNSSEC org
http://www.dnssec.org/

Sources and references for Stefan Björk-Olsén

Signature-based antivirus is dead: get over it
by Liam Tung
Written/Posted: Wednesday, April 30, 2008 09:28 AM
Last accessed on 11may 2008
http://www.zdnetasia.com/news/security/0,39044215,62040791,00.htm

Are 'Good' Computer Viruses Still a Bad Idea?
by Research Associate, Virus Test Center
Unknown when written and posted.
Last accessed on 12may 2008
http://vx.netlux.org/lib/avb02.html

Virus Timeline
by Joe Wells
Written/Posted: 30 August 1996
Last accessed on 12may 2008
http://www.research.ibm.com/antivirus/timeline.htm

How computer viruses works
by Marshall Brain
Unknown when written and posted.
Last accessed on 11may 2008
http://www.howstuffworks.com/virus.htm

What is a Virus Signature?
by Mary Landesman
Unknown when written and posted.
Last accessed on 11may 2008
http://antivirus.about.com/od/whatisavirus/a/virussignature.htm

The Cross-site Scripting Virus
by Wade Alcorn
Published: 27th September 2005
Last Edited: 16th October 2005
Last accessed on 12 may 2008
http://www.bindshell.net/papers/xssv/

Antivirus
by Dmoz
Unknown when written and posted.
Last accessed on 12may 2008
http://www.dmoz.org/Computers/Security/Malicious_Software/Viruses/

Defcon Race to Zero contest angers antivirus vendors
by "Matthew"
Written/Posted: 29april 2008
Last accessed on 11may 2008
http://www.geek.com/defcon-race-to-zero-contest-angers-antivirus-vendors/

Need a computer virus?- download now
by infoniac
Written/Posted: 22 May 2007
Last accessed on 12may 2008
http://www.infoniac.com/offbeat-news/computervirus.html

The Future of Antivirus [1]
by Michael Fitzgerald
Written/Posted: 03 Mars 2008
Last accessed on 11 May 2008
http://www.csoonline.com/article/221324

Dancho Danchev's
by Dancho Danchev
Written/Posted: 06 Mars 2008
Last accessed on 12 May 2008
http://ddanchev.blogspot.com/

Security Vendors Slam Defcon Virus Contest
by Robert McMillan, IDG News
Written/Posted: 25 April 2008
Last accessed on 11may 2008
http://www.pcworld.com/businesscenter/article/145148/security_vendors_slam_defcon_virus_contest.html

Some of these sources may, if you look from a strict scientific perspective, look 'unprofessional' due to the fact that they seem to be 'random' internet pages rather then scientific papers. This is due to that a lot of the information we like to present in this paper are first of all new, to reflect the current status of antivirus, some written only late the month before or early in the month in which this paper was written. Second of all we like to make our own assumptions and ideas rather then basing them on another paper.

As a last note I would just like to say that some of the information in this paper comes from our own knowledge and conclusion so certain parts will reflect our views and knowledge of the antivirus scene. So the information in this paper should not be used as a reference but rather a summary of the information available on Anti-viruses. If you are interested in Anti-virus and wishes to read more we recommend you start by reading our sources posted above.

We hope that you liked this paper and any questions may be directed to us at steffe_b@hotmail.com .

Sources and references for Martin Hafstrand

Title: W32.Blaster.Worm
Author: Douglas Knowles, Frederic Perriott
Discovered: August 11, 2003
Updated: December 9, 2003 11:50:19 PM
http://www.symantec.com/security_response/writeup.jsp?docid=2003-081113-0229-99&tabid=2

Title: The 10 Most Destructive PC Viruses Of All Time
Author: By George Jones, TechWeb
http://www.techweb.com/article/showArticle.jhtml;jsessionid=K14TMXCLXFPJMQSNDLPCKH0CJUNN2JVN?articleId=160200005&pgno=2

Main title: Antivirus Research and Detection Techniques
Title: Introduction
Author: Jay Munro
Date: Jul 5, 2006 09:00 AM
http://www.extremetech.com/article2/0,2845,325439,00.asp

Title: Definitions
http://www.extremetech.com/article2/0,2845,1153277,00.asp

Title: Research, Research, and More Research
http://www.extremetech.com/article2/0,2845,1154644,00.asp

Title: Detection Method Overview
http://www.extremetech.com/article2/0,2845,1154645,00.asp

Title: Viral History
http://www.extremetech.com/article2/0,2845,1154646,00.asp

Title: Finding Today's Viruses with Signature Scanning
http://www.extremetech.com/article2/0,2845,1154647,00.asp

Title: Generic signatures
http://www.extremetech.com/article2/0,2845,1154648,00.asp

Main title: Antivirus Research and Detection Techniques, Part II
Title: Heuristic Scanning
http://www.extremetech.com/article2/0,2845,367051,00.asp
Title: Polymorphic and Metamorphic Detection
http://www.extremetech.com/article2/0,2845,1166168,00.asp

Title: Mobile viruses, a ticking bomb
Author: Zam Karim
Date: Thursday April 24, 2008
http://star-techcentral.com/tech/story.asp?file=/2008/4/24/itfeature/1059075&sec=itfeature*