Frank R. Chapman
Thomas R. Smith
CHAPMAN VALDEZ
PO Box 2710
Casper, Wyoming 82602
(307) 237-1983
(307) 577-1871 (fax)
ATTORNEYS FOR DEFENDANT

In The District Court

For the District of Wyoming

UNITED STATES OF AMERICA,)
)
Plaintiff,)
)
vs.) Case No. 07-CR-32-B
)
NATHANIEL SOLON)
)
Defendant.)

STATE OF WYOMING)
) ss.
COUNTY OF NATRONA)

AFFIDAVIT OF ROBERT REILLY

The undersigned, Robert Reilly, being of lawful age and being first duly sworn upon his oath, deposes and states as follows:

1. I have many years experience with computers, having first worked with such old computers as the Commodore 64. I have Global A+ Certification in Computer Electronics, through the Computer Technology Industry Association, Verification # 901DTT1252; Candidate # 076AFI. I am a Microsoft Partner, provide MicroSoft 24/7 Critical Business Support, and regularly attend MicroSoft training. I have been involved in running computer businesses for

approximately 12 years, including Calvary Computers in Casper, Wyoming. I currently have two jobs in the computer industry, including managing and owning MicroTechnology Consulting and MicroTechnology Leasing. I am a computing technologist or technical adviser and IT manager, managing global networks. Through the technology groups, we assist companies such as Home Depot, Office Max, Pizza Hut, Taco Bell, Circuit City, Sears, Woodward Steering Company, as well as many local companies. Among other things, I provide solutions to problems people and companies have with their computer systems and networks. Additionally, I provide ISP services to businesses

2. I know Nathaniel Solon and have been acquainted with him for many years. I consider him a family friend.

3. I have familiarity with a computer he owned in the year 2006. Building personal computers for home use is not what I usually do, but because Ned is a friend, I built his computer for him and serviced it on a number of occasions. Ned often bought used equipment. During the times in 2006 when I serviced his computer, I never saw any indication of child pornography.

4. After his hard drive was seized in September, 2006, I partially rebuilt his computer and then returned it to him. I do not have records of everything I did as a part of that rebuild.

5. I have been asked my opinion of certain evidence regarding the existence of child pornography on the hard drive seized from Ned. It is my understanding that Ned's hard drive was seized without the rest of the system being seized. I have seen printouts of digital information present on Ned's drive.

6. It is my opinion that a proper analysis of what was viewable on Ned's computer prior to it being seized is impossible or extremely difficult at the present time because of the lack of seizure of the entire computer. This is so for at least the following reasons:

Lack of being able to log in to the active partition prevents us from seeing all files. Several files are locked by the operating system when the hard drive is removed from the hardware system it was originally connected to. And while we are able to force control of this data from a server platform, with removal of the hard drive, certain algorithms are necessarily changed the moment the drive is brought up on another system.

Put another way, in my opinion, it is impossible to tell, with only the hard drive, what was actually viewable on Ned's computer when it was seized. The presence of data viewable on another system does not mean it was viewable on Ned's system.

I have seen a log file containing names of files, but not enough to get an accurate determination of what was happening.

In my opinion, it is quite possible that what appear, by name, to be "child pornography" files, could have been sent to Ned's hard drive by one of dozens of viruses. Some viruses are specifically meant to take control of user's computers without knowledge nor consent.

By way of example only, and not exclusively, in a simple search on the TrendMicro website, using "Madden" as a search term (chosen because "Madden" appears on the log file) there were listed warnings of numerous viruses, some of which allowed non-local users (not Ned, someone from a remote location) complete control of user's (Ned's) computer. (See attached)

The possibility of a virus is only one area of concern that is incapable of complete analysis with only the hard drive or hard drive image.

A computer system is just that, a system. A proper analysis of what the system is capable of doing cannot be done with one component of the system.

FURTHER, YOUR AFFIANT SAYETH NAUGHT.

DATED this 13 day of April, 2007.

Robert Reilly

STATE OF WYOMING)
) ss.
COUNTY OF NATRONA)

Subscribed and sworn to before me by ROBERT REILLY, this 13th day of April, 2007.

WITNESS my hand and official seal.

Marla Heberlein
NOTARY PUBLIC

MY COMMISSION EXPIRES:

NOTARY PUBLIC
MARLA HEBERLEIN
STATE OF WYOMING
COUNTY OF NATRONA
My Commission Expires Mar 17, 2010

TREND MICRO

Virus Encyclopedia Search Results
<< Search Again

1 - 10 of 23 record(s) match your query

MADDEN

MADDEN-B

WORM_IXBOT.A
Aliases: Backdoor.IRC.Bot, W32/IRCbot.worm
This memory-resident worm spreads via popular instant messaging applications like the following: AOL Instant Messenger (AIM) AOL Triton MSN Messenger When exe...

WORM_SDBOT.I
Aliases: W32/Sdbot.worm, Win32/SDBot!Backdoor!Server.Variant!Trojan
The malware attempts to propagate by dropping copies of itself in the shared folders of the following peer-to-peer applications installed on an infected system: Kazaa iMesh ...

WORM_SPECX.B
This memory-resident malware has both worm and backdoor capabilities. It propagates via peer-to-peer (P2P) application such as Kazaa and iMesh. It performs the following actions on a target...

WORM_SPYBOT.BK
Aliases: Backdoor.Sdbot.gen
This memory-resident worm propagates via peer-to-peer applications, specifically Kazaa and Imesh. It has the following capabilities: Can act as an Internet Relay Chat (IRC) bot ...

WORM_FRANRIV.A
This worm is a proof-of-concept program, which demonstrates how a game construction kit, such as the popular Game Maker, can be used maliciously. The program supports registry and file manipulation...

WORM_SHYNET.B
Aliases: W32.HLLW.Shydy.B, Worm.P2P.VB.ag
This nondestructive variant of WORM_SHYNET.A worm attempts to propagate via file-sharing networks such as ...

WORM_SHAREBOT.A
This worm propagates by dropping copies of itself in shared folders with Read or Read/Write access in the root and Windows directory. It uses ...

WORM_SPYBOT.H
Aliases: W32/Spybot.H.worm
This worm spreads via the Kazaa peer-to-peer file-sharing network. It also acts as a backdoor and connects to a certain IRC (Internet Relay Chat) server. Through IRC, it is able to receive commands...

Result page : 1 2 3 Next

› Search for madden in **all Trend Micro pages**
› Search for madden in our **Knowledge Base**

TREND MICRO

Virus Encyclopedia Search Results

<< Search Again

11 - 20 of 23 record(s) match your query

WORM_TIBICK.A
Aliases: W32.Tibick, W32/Tibick.C@p2p, Win32.Tibick.E, Worm:Win32/Tibick.D
This worm propagates via peer-to-peer (p2p) networks by dropping copies of itself into shared folders used by p2p applications, such as Kazaa. It uses attractive file names t...

WORM_TIBICK.B
This worm propagates via peer-to-peer (P2P) applications. It drops copies of itself using attractive names into the folder %Windows%\msview.exe, which it later on registers as the shared fol...

WORM_TIBICK.C
This worm propagates via peer-to-peer (P2P) applications. It drops copies of itself using attractive names into the folder %Windows%\msview.exe, which it later on registers as the shared fo...

WORM_LACON.A
Aliases: W32.HLLW.Lacon@mm, W32/Nocall.A, Win32.HLLM.Generic.219, Win32:HLLM-Generic [Wrm]
This memory-resident worm propagates via email, Internet Relay Chat (IRC), and file-sharing networks such as Kazaa, Kazaa lite, Bearshare, Edonkey2000, Morpheus and Limewire. It sends copies...

WORM_AGOBOT.02H
Aliases: W32/Gaobot.worm
This worm propagates via network-shared drives and file-sharing networks such as Kazaa, Grokster, and Bearshare. It is designed to connect to an Internet Relay Chat (IRC) server and acts as an IRC bot...

WORM_AGOBOT.B
Aliases: GAOBOT.A, W32/Gaobot.worm, Backdoor.Agobot.01
This worm propagates via Kazaa (a peer-to-peer application) as well as network shared drives. It attempts to connect to an IRC server and act as a bot that can be used to launch a Denial of Service...

WORM_AGOBOT.C
Aliases: W32/Gaobot.worm.j, Backdoor.Agobot.040, Backdoor:Win32/Agobot.0_40, Win32.Agobot.040.A
This memory-resident worm propagates via the Kazaa, Grokster and Bearshare file-sharing networks and network shared drives. It regularly attempts to connect to an Internet Relay Chat (IRC) server a...

WORM_AGOBOT.D
Aliases: Backdoor/Agobot, Win32/HLLW.Gaobot
This memory-resident worm, related to WORM_AGOBOT.C, propagates via the Kazaa, Grokster, or Bearshare file sharing networks and via network shared drive...

WORM_AGOBOT.E
Aliases: W32/Gaobot.worm, W32.HLLW.Gaobot, W32/Agobot.B (exact), Worm.P2P.Agobot.b, Win32/HLLW.Agobot.B
This worm propagates via the Kazaa peer-to-peer file-sharing network and via network shared drives. It attempts to connect to an Internet Relay Chat (IRC) server and act as a bot program that can be u...

WORM_AGOBOT.F
Aliases: BDS/Agobot.015.F, W32/Gaobot.worm, Worm/Agobot, Win32.Agobot.C
This worm propagates via the Kazaa peer-to-peer file-sharing network and via network shared drives. It attempts to connect to an Internet Relay Chat (IRC) server and act as a bot program that can be u...

Result page : Previous 1 2 3 Next

› Search for madden in **all Trend Micro pages**
› Search for madden in our **Knowledge Base**

TREND MICRO

Virus Encyclopedia Search Results

<< Search Again

21 - 23 of 23 record(s) match your query

WORM_AGOBOT.G

Aliases: Worm.Win32.Agobot.104448.E, Backdoor.Agobot.02.k, Win32.HLLW.Zombot.2

This worm is designed to propagate via the Kazaa peer-to-peer file-sharing network and via network shared drives. It attempts to connect to an Internet Relay Chat (IRC) server and act as a bot prog...

WORM_DIOXIN.B

Aliases: Malware.d

This memory-resident worm spreads by sending a message to any available or online contacts listed in an affected user's AOL Instant Messenger (AIM). The said message contains a link, which w...

WORM_SDBOT.JA

This memory-resident malware has both worm and backdoor capabilities. It arrives as an infected file via common peer-to-peer (P2P) applications such as Kazaa, Morpheus, Grokster, BearShare, eDonkey...

Result page : Previous 1 2 3

› Search for madden in **all Trend Micro pages**

› Search for madden in our **Knowledge Base**

TREND MICRO

Global Sites
日本語 繁中 简中 대한민국

Home | Products & Services | Purchase | Support | Security Info | Partners | About Us | Find a product

Knowledge Base
› Search Tips
› Submit Question

FAQs

Update Center

Supported Versions

Beta Programs

Virus Response Service

Submission Wizard

Premium Support

Online Registration

Welcome Customer

Knowledge Base Search

Enter issue or solution ID	madden Example: My patch install fails
Choose your Product:	All
Version	All
Document Type:	All

Advanced Search

Results for: "madden" Save Search

24 results found **Sort By:** Most Recent

Search Results: 1 to 24

WORM_FRANRIV.A
This worm is a proof-of-concept program, which demonstrates how a game construction kit, such as the popular Game Maker, can be used maliciously. The program supports registry and file manipulation and even the execution of any program. Due to bugs in its code, however, the worm program may not run properly. It propagates via the popular peer-to-peer file sharing network Kazaa and requires that the folder C:\Windows exists before it executes. As a result, it may not run on Windows NT and 2000, since the folder is not found on typical installations of these platforms. Note, however, that this worm can execute smoothly on Windows 95, 98, ME, NT, 2000, and XP machines that have the folder C:\Windows. This worm displays either of the following messages, depending on the outcome of its intended routines: Note that TrendLabs does not consider or detect game construction programs per se, as malicious. But due to certain features, it may be utilized maliciously.

2/26/06
WORM_IXBOT.A
This memory-resident worm spreads via popular instant messaging applications like the following: AOL Instant Messenger (AIM) AOL Triton MSN Messenger When executed, this worm sends a message to the affected user&apos;s instant messenger contacts. The message contains a link, which when clicked, downloads a copy of this worm to the recipient&apos;s system. It uses the affected user&apos;s ID to send messages to target contacts. This may lead unsuspecting recipients to most likely click on the link since it came from a known source. Deception doubles because it even has the ability to reply to messages sent to it. It also has backdoor capabilities. It connects to a certain port. Once connected, a remote malicious user now has the capability to

Personalized Su
› Need to Regist
› Login

Refine Your Sea

Activity:
› Delivering Em
› Generate Logs
› Detecting Cert Infected (3)
› Determining V Microsoft Winc
› Local Server (
more...

Topic:
› Mail Abuse Pre System (8)
› Network Repu Service (8)
› Open Proxy St
› RBL+ Service
› Outbreak Prev (8)
more...

System:
› Microsoft Fligh (10)
› Microsoft Offic
› Microsoft Links
› Symantec Nor (8)
› Adobe Acrobat
more...

download and execute files. This capability compromises the system&apos;s security. Moreover, it drops many copies of itself, which have enticing file names related to games, system tools, and other popular applications. Disguising itself with attractive file names tricks the user into thinking that the files are legitimate. This worm disables certain antivirus applications from running during every system startup by deleting certain registry entries. This routine makes the affected system very vulnerable to malicious attacks.

12/8/05
WORM_DIOXIN.B
This memory-resident worm spreads by sending a message to any available or online contacts listed in an affected user&apos;s AOL Instant Messenger (AIM). The said message contains a link, which when clicked, downloads a copy of this worm into the target system. It uses the affected user&apos;s AIM Screen Name or user ID, and is even capable of replying to instant messages sent to it. Thus, unsuspecting users may think that the link comes from a trusted source and proceed to download the worm copy into their machines. This worm also propagates through peer-to-peer (P2P) file sharing networks by dropping copies of itself into folders related to popular P2P applications. Its dropped copies use attractive file names related to games, system tools, and other popular applications, thus tricking users into thinking that the said files are legitimate. This worm has backdoor capabilities that may allow a remote malicious user to gain control over the affected machine. Moreover, it disables several system tools and changes system settings. It also displays the following messages when executed:

12/8/05
WORM_TIBICK.C
This worm propagates via peer-to-peer (P2P) applications. It drops copies of itself using attractive names into the folder % Windows%\msview.exe , which it later on registers as the shared folder for various P2P programs, such as DC++, eMule, Imesh, Kazaa, and Morpheus. It has backdoor capabilities. It connects to an Internet Relay Chat (IRC) server and waits for a command from a remote user to download and execute files from the affected system. This worm runs on Windows 98, ME, NT, 2000, and XP.

5/6/05
WORM_TIBICK.A
This worm propagates via peer-to-peer (p2p) networks by dropping copies of itself into shared folders used by p2p applications, such as Kazaa . It uses attractive file names to entice users to download and execute copies of itself into their systems. This worm has backdoor capabilities. It connects to a certain IRC server and waits for commands coming from a remote malicious user. It can then execute remote shell commands and relay information about the infected system to the remote user.

3/10/05
WORM_AGOBOT.D
This memory-resident worm, related to WORM_AGOBOT.C , propagates via the Kazaa, Grokster, or Bearshare file sharing

Issue:

› Windows Mess

networks and via network shared drives. It regularly connects to an Internet Relay Chat (IRC) server as a bot, allowing its remote user to launch a Distributed Denial of Service (DDoS) attack from infected machines. This worm, which affects systems running Windows NT, 2000, and XP, also has backdoor server capabilities and can allow remote users to access and manipulate infected systems. It sends out a notification to its remote user that can contain sensitive information, including application serials and IP addresses.

2/26/05
WORM_SDBOT.I
The malware attempts to propagate by dropping copies of itself in the shared folders of the following peer-to-peer applications installed on an infected system: Kazaa iMesh It has backdoor capabilities which allow malicious remote users to do the following: Send email messages using a built-in SMTP engine Parse the registry for Serial numbers and CD keys of some computer games Perform denial of service (DoS) attack against other systems Upload / Download file(s) List and terminate running processes List system information Browse files on the compromised system Execute a file remotely This malware runs on Windows 95, 98, ME, NT, 2000 and XP. It is compressed using Aspack and is encrypted using EXE Stealth. Due to the complexity of the stealth mechanism employed, most of its routines are not carried out.

12/5/04
WORM_SHAREBOT.A
This worm propagates by dropping copies of itself in shared folders with Read or Read/Write access in the root and Windows directory. It uses file names that can trick users into thinking they are crack programs for certain software. It also attempts to modify the registry settings of popular file-sharing services. This worm also attempts to connect to an mIRC server to notify a remote user and listen for further commands. It runs on Windows 95, 98, ME, NT, 2000, and XP.

11/22/04
WORM_TIBICK.B
This worm propagates via peer-to-peer (P2P) applications. It drops copies of itself using attractive names into the folder % Windows%\msview.exe , which it later on registers as the shared folder for various P2P programs, such as imesh , DC++ , mopheus , and emule . (Note: %Windows% is the Windows folder, which is usually C:\Windows or C:\WINNT.) It has backdoor capabilities. It connects to an Internet Relay Chat (IRC) server and can receive command from a remote user to download and execute files. It runs on Windows 95, 98, ME, NT, 2000, and XP.

11/15/04
WORM_SPECX.B
This memory-resident malware has both worm and backdoor capabilities. It propagates via peer-to-peer (P2P) application such as Kazaa and iMesh. It performs the following actions on a target machine: Drop itself as the file IEXPLORE32.EXE in the Windows system folder Create a directory and attempts to copy itself using specificl file names Connect to an Internet Relay Chat (IRC) server and join a certain channel Allow a remote

malicious user to execute the following commands: Terminate process Display system and network information Send email Create clones Redirect connection Initiate SYN, Ping, or UDP flood to launch a Denial of Service (DoS) attacks Execute file Steal CD keys Attempt to connect to certain servers Display a fake message box upon execution Terminate several programs, which are running on the system This malware is compressed using ASPack and ExeStealth. It runs on Windows NT, 2000, and XP.

1/15/04

WORM_SDBOT.JA

This memory-resident malware has both worm and backdoor capabilities. It arrives as an infected file via common peer-to-peer (P2P) applications such as Kazaa, Morpheus, Grokster, BearShare, eDonkey2000, iMesh, and Limewire. It performs the following tasks on a target machine: Drop a copy of itself as the file MSNQMGR.EXE in the Windows system directory Connect to an Internet Relay Chat (IRC) server and join a specific channel Listen for and execute commands from a remote user as follows: Upload and download files Create clones Execute files It searches for the locations of commonly used P2P file-sharing software. When the said programs are found, this malware attempts to copy itself to the default shared file locations using certain file names. Otherwise, it drops a copy of itself in the My Music folder, which is usually located in My Documents directory. This worm is compressed using a modified UPX and runs on Windows 95, 98, ME, NT, 2000, and XP.

1/15/04

WORM_SPYBOT.BK

This memory-resident worm propagates via peer-to-peer applications, specifically Kazaa and Imesh. It has the following capabilities: Can act as an Internet Relay Chat (IRC) bot Attempt to connect to a particular Web site using a specified user name Send system information as follows: Processor Total size of memory Free memory Operating system Uptime Connection type IP address User name Steals CD keys of several software Terminate several applications, which includes antivirus products, and firewall programs This Aspack-compressed malware is written in Visual C++, a high-level programming language, and only runs on Windows XP.

12/14/03

WORM_SPYBOT.H

This worm spreads via the Kazaa peer-to-peer file-sharing network. It also acts as a backdoor and connects to a certain IRC (Internet Relay Chat) server. Through IRC, it is able to receive commands from a remote malicious user to process on the compromised machine. It is capable of executing the following actions: Log keystrokes Steal cached passwords Perform denial of service (DoS) attacks against other hosts List and terminate running applications Download, modify and execute files Create directories Retrieve system information Scan ports Control the CD-Rom tray It runs on Windows 95, 98, ME, NT, 2000 and XP.

10/14/03

WORM_LACON.A

This memory-resident worm propagates via email, Internet Relay Chat (IRC), and file-sharing networks such as Kazaa, Kazaa lite, Bearshare, Edonkey2000, Morpheus and Limewire. It sends copies of itself to all addressess in the Web Address Book (WAB). The message that it sends out has the following details: Subject: National No Call Registry Info Message Body: (Any of the following) You&apos;ve probably heard about the National No Call Registry to stop telemarketers. Well I tried it just yesterday and so many people are using it I couldn&apos;t get through. But good news, they just issued this program to automate everything, check the attachment! Love ya! Finally they created a program to stop those annoying telemarketers, it adds you to the National No Call Registry automatically. Check the attachment! Keep in touch! Get added to the National No Call List to make it illegal for telemarketers to call you, just click the attachment to add yourself. Talk to you later! I just saw this on the local news. You can add yourself to this National No Call List so telemarketers stop calling. I just did it, its real easy. Just click the attachment to add yourself! See you soon! Attachment: No Call List.exe It runs on Windows 95, 98, ME, NT, 2000, and XP systems.

9/3/03

WORM_SHYNET.B

This nondestructive variant of WORM_SHYNET.A worm attempts to propagate via file-sharing networks such as Kazaa and iMesh. However, due to errors on its code, it fails to execute some of its routines. It is written in Visual Basic and usually arrives compressed under the UPX compressor software. It runs affects systems running on Windows 95, 98, ME, NT, 2000 and XP.

8/22/03

WORM_AGOBOT.G

This worm is designed to propagate via the Kazaa peer-to-peer file-sharing network and via network shared drives. It attempts to connect to an Internet Relay Chat (IRC) server and act as a bot program. As a IRC bot, this worm can be used by remote users to launch a Denial of Service (DoS) attack against other users. It is also designed with backdoor server capabilities, allowing remote users to access and manipulate infected systems. Errors in this worm&apos;s code causes it propagation routines to fail. This worm runs on Windows 95, 98, ME, NT, 2000, and XP.

7/12/03

WORM_AGOBOT.02H

This worm propagates via network-shared drives and file-sharing networks such as Kazaa, Grokster, and Bearshare. It is designed to connect to an Internet Relay Chat (IRC) server and acts as an IRC bot that allows its remote user to launch a Distributed Denial of Service (DDoS) attack against target machines. This worm is also designed to have backdoor server capabilities that allow remote users to access and manipulate infected systems. It runs on Windows 95, 98, NT, ME, 2000 and XP systems.

5/20/03

WORM_AGOBOT.F

This worm propagates via the Kazaa peer-to-peer file-sharing network and via network shared drives. It attempts to connect to an Internet Relay Chat (IRC) server and act as a bot program that can be used to launch a Denial of Service (DoS) attack against other users. This worm is designed to have backdoor server capabilities that allow remote users to access and manipulate infected systems. This worm runs on Windows 95, 98, NT, 2000, ME, and XP.

4/27/03

WORM_AGOBOT.E

This worm propagates via the Kazaa peer-to-peer file-sharing network and via network shared drives. It attempts to connect to an Internet Relay Chat (IRC) server and act as a bot program that can be used to launch a Denial of Service attack against other users. This worm is designed to have backdoor server capabilities that allow remote users to access and manipulate infected systems. This worm runs on Windows 95, 98, ME, NT, 2000, and XP.

4/11/03

WORM_AGOBOT.C

This memory-resident worm propagates via the Kazaa, Grokster and Bearshare file-sharing networks and network shared drives. It regularly attempts to connect to an Internet Relay Chat (IRC) server as a bot. When connected, it may be used to launch Denial of Service (DoS) attacks against other users. This worm also has backdoor server capabilities and enables remote malicious users to access and manipulate infected systems. This worm works on Windows NT, 2000, and XP.

12/6/02

WORM_AGOBOT.B

This worm propagates via Kazaa (a peer-to-peer application) as well as network shared drives. It attempts to connect to an IRC server and act as a bot that can be used to launch a Denial of Service attack against other users. This worm may also have backdoor server capabilities and may allow remote users to access and manipulate infected systems.

11/10/02

MADDEN-B

9999 MADDEN-B. File Infector. 1440 bytes. 2.062 or later. 0.518.00 0 Y. 1999-03-31 00:00:00.0. 2000-03-09 13:45:50.0. 2000-03-09 13:45:49.683. 0 Execution Procedure: Searches for an uninfected EXE file and infects it. The searching path is from the current directory to its

5/3/08

MADDEN

9998 MADDEN. File Infector. 1988 bytes. 2.062 or later. 0.518.00 0 Y. 1999-03-31 00:00:00.0. 2000-03-09 13:45:50.0. 2000-03-09 13:45:49.683. 0 Execution Procedure: Searches for an uninfected EXE file and infects it. The searching path is from the current directory to its

5/3/08

WORM_SPYBOT.CX

This memory-resident worm propagates via network shares and

Kazaa, a popular peer-to-peer file sharing application. It drops copies of itself in a folder it creates, using interesting file names to entice users to download the files. This malware also attempts to access network shares and drop a copy of itself in the shared folder, using a long list of passwords for its logon credentials. It has the ability to do a denial of service attack in any location that a remote malicious user chooses. It also has backdoor capabilities, such as listening to random ports, waiting for a connection from a remote user, and compromise a target machine. It runs on Windows 95, 98, ME, NT, 2000 and XP.

7/27/06

✉ Email this page — ★ Rate this page —

Legal Notice | Privacy Policy | Contact Us