The Computer Link

May 2001

The Newsletter of the Northern Neck Computer Users' Group

NNCUG Officers

Al Brittle, Pres.
(804) 462-7023
brittle@crosslink.net

Jim Sapione
(804) 462-5831
jsapione@crosslink.net

Camille Bennett, Sec'y
(804) 435-1929
cbennett@rivnet.net

John Parr, Treasurer
(804) 333-3867
parr@crosslink.net

Jim Talbot
(804) 580-6692
jftmmt@rivnet.net

The Computer Link
Betty Lehman, Editor
435-2011
blehman@crosslink.net

Jerry Lehman,
Associate Editor
gbdev@crosslink.net

NNCUG URL:
http://www.
nncug.org

Send Newsletter
submissions to:
blehman@crosslink.net
➔DEADLINE➔
for NEXT ISSUE,
15th of MONTH

IF YOU THINK VIRUSES COME *ONLY* IN ATTACHMENTS, THINK AGAIN.

Virus Alerts
Wednesday, March 14, 2001

Magistr: A Recipe Of Blending Virus and Worm with some Multilevel Polymorphism Flavour
Cambridge, United Kingdom, March 14, 2001; Kaspersky Labs, an international data-security software-development company, warns computer users about the discovery of a new extremely dangerous computer virus "Magistr," which spreads via e-mail and local area networks, and uses a set of nifty techniques to hide its presence in infected computers that makes it very difficult to detect and disinfect. According to the comments found in the virus body, it was written in Malmö, Sweden by hacker going by the pseudonym of "The Judges Disemboweler." Kaspersky Lab has already received several reports about the worm "in-the-wild." "Magistr" can enter a computer three ways: firstly, via e-mail messages when a user has accidentally launched the infected attached file; secondly, using the local area network (LAN) by infecting files found on available servers and workstations; shared resources; thirdly, when an infected file has been delivered to a system by any removable storage media or downloaded from the Internet or other networks. Right after the infected file is executed, the virus initiates the procedure of penetration into the system, mass e-mail distribution and, after some time, it activates the built-in destructive payload. To complete the mass e-mail distribution, "Magistr" scans the Outlook Express, Internet Mail and Netscape Messenger mail databases and Windows address book, and reads all e-mail addresses.

Details about the mail databases location and their names are stored in a special file having the DAT extension. The name of the file is derived by encrypting the original computer's name. For instance, if a computer has a name CS-GOAT, then the file will be named WG-SKYF.DAT. Depending on the first character of the filename, the virus copies this file in the C: drive root directory or the "Windows" or "Program Files" directory.

After this, "Magistr" invisibly retrieves the SMTP server that is connected to the infected computer, and, on behalf of the user, sends out e-mail messages through the server containing random PE, EXE or SCR files less than 132Kb in size that are already infected with the virus. The subjects of the messages are randomly selected from DOC and TXT files found on the computer or from the list of some English, Spanish and French phrases planted in the virus body. The body of the messages contains no text. Such inconstancy of outward appearance of the distributed e-mails significantly complicates the identification of infected e-mails by users themselves.

It is important to note that when sending out infected e-mails, "Magistr" randomly changes the sender's return address by deleting or changing some characters. This fact also helps the virus hide its activity, since the recipient cannot answer the message because of an incorrect return address. Thus, the sender is not able to ascertain that the virus is sending out unauthorized messages from his or her computer. Right after the virus code is executed, "Magistr" infects all PE EXE and SCR files found in "Windows," "WinNT," "Win95" and "Win98" catalogues of all local and network drives connected to this particular computer. After this, the virus scans all available network resources, looks for the aforementioned catalogues, and infects PE EXE and SCR files there. When infecting the files, "Magistr" uses several very sophisticated techniques that significantly complicate its detection and removal. The virus is divided into three parts with

(Continued on page 2)

(Continued from page 1) If you think………..

two of them encrypted with a strong polymorphic algorithm, so the infected file appears in the following way: Therefore, after the infected file is run, the virus immediately intercepts its execution in the program's entry point, and redirects the program's processor to the main virus code. Only after the main virus code has been completed does the virus return control to the original program. In order to secure its constant presence in the infected systems, "Magistr" modifies the WIN.INI configuration file and Windows system registry in a way that the virus is activated each time the system boots up. When infecting network resources, the virus modifies the WIN.INI file only. "Magistr" carries a very dangerous destructive payload. One month after the day of the first infection, the virus destroys all files on local and network drives on computers running Windows NT/2000 by replacing their original contents with the string "YOUARE ____ ". Under Windows 95/98, the virus additionally discards the CMOS memory settings (CMOS contains the computer boot up hardware settings) and, just like the "Chernobyl" (CIH) virus, destroys data in FLASH BIOS microchip. After this, it displays the following message box: " Another haughty bloodsucker....... YOU THINK YOU ARE GOD , BUT YOU ARE ONLY A CHUNK OF ____ ". Depending on the internal triggers, the virus also executes yet another payload subroutine that invokes the "runaway icons" effect: if a user tries to point the cursor to a desktop icon, the icon immediately changes its location so the user cannot start the correspondent application:

"In this particular case, we are dealing with a very complex and technologically advanced computer virus, which is powered by all the most effective ways of spreading, infection, masquerading and has a very dangerous payload," said Denis Zenkin, Head of Corporate Communications for Kaspersky Lab. "As a matter of fact, "Magistr", is a result of the successful crossing of the outstanding spreading speed of the "ILOVEYOU" virus and "Chernobyl's" extreme destructiveness." Taking into account the danger and breath-taking spreading of the "Magistr" virus, Kaspersky Lab recommend its users update the Kaspersky Anti-Virus anti-virus database as soon as possible. Protection against the virus has already been added to the program's daily update. Kaspersky Anti-Virus can be purchased in the Kaspersky Lab online store or from a worldwide network of Kaspersky Anti-Virus distributors and resellers.

E-mail: denis@kaspersky.com; http://www.kaspersky.com;
http://www.viruslist.com
Secure Your Cyberspace with Kaspersky Anti-Virus (AVP)!

A BRIEF HISTORY *of my computer encounter (if anyone cares)*....................by Betty Lehman, editor

In 1992, I purchased a computer. The range of computer performance at that time ranged between the 286 and 486 chipset . I chose 386/40 mhz. After reading the pros and cons of Intel or American Microdevices (AMD) chipsets and their many foreign imitators, I picked AMD. I think both of the major chipsets would have been equal. The memory I opted for was 32 Mg RAM. I had a 3.5" floppy drive, a 5.5" floppy drive a 125 Mg. IDE hard drive, a Trident Video Card with 1 Mg RAM (even video cards need RAM), an internal Modem (14,400 bps) and a 15" Monitor with 1024 X 768 Max resolution. The package also came with a Citizen dot matrix black and white printer 360 X 360 DPI Resolution. This last was priced at $309.95. The total cost of my new system was $2091. 57.

Now all this might not mean too much to those who have not yet begun their acquaintance with the electronic world. It didn't mean a whole lot to me either although I had attended meetings at the Northern Neck Computer Users Group for several months, letting the jargon flow around me 'til it began to sink in. The newcomer to computing today has a much larger field to explore in the packages produced under a zillion different trademarks. The prices have come down greatly, and the capabilities have improved immensely.

My personal computer looks much the same as it did when I purchased it. The housing is the same mid-tower-sit-on-the-floor cabinet, although the interior has been completely redecorated. The newest mother board has a Pentium 450 chipset, and 128 Mg. of RAM. It sports a CD-ROM drive, and a CD-RW drive. I have a zip drive, a scanner, a color inkjet printer, and a laser printer (B/W). A new monitor was added a couple of years back due to failure of the original, and a new keyboard for the same reason. My original mouse died and subsequent mice have joined the troop. The modem was upgraded to 56 k for optimum internet activity, and even the power supply has been replaced. I am quite content, at present, with the overall performance. Windows 98 SE is the operating system of choice for me at this time, and Norton 2001 anti-virus software keeps things clean.

A computer can be useful for making the checkbook register legible. My handwriting has deteriorated over

(Continued on page 3)

(Continued from page 2) A Brief History………..

the last ten years and finding record of checks written for subscriptions, donations, bill payments, to verify their payment or to determine that it hasn't been duplicated is not as easy as it once was. It is a good method of checking your balances also, although Quicken's "reconciling" is still a bit tricky for me.

I correspond with our three sons and their children, in Arizona, Connecticut, and New Hampshire respectively, and send faxes for my husband's business correspondence, after scanning papers into the computer.

A newsletter published monthly by our computer group is composed on my computer, and after printing it on the inkjet printer at best resolution, it is delivered to Kinkos for mass production by photocopy in black and white. Color copies are still very dear. But since I do the original in color, when it is forwarded to our Website, nncug.org, folks can see it in all its glory.

The internet is a great place to review movies and nearby theatres. You can even see a map if you are not familiar with the location of a theatre you wish to visit.

Recently a Special Interest Group was formed by our computer users group to help research into Genealogy and it stimulated an interest in me to find my husband's European family connections. Fortunately my mother did much research on her family background and on my father's, so I won't have to. This activity can take up a whole lot of time, however, and in my world, time is extremely valuable.

I was able to find the manufacturer of a bird feeder I have to replace one perch which had broken. This they did without charge after I contacted their website. I also located the distributor of a hair product I am fond of and which I have to go to a city mall when I need it. Of course, shipping and handling must be added to the cost but it's worth not having to drive in to Richmond.

Shopping for vacation spots is another favorite activity for many, although we prefer to use the services of a local travel agency to hammer out the details. One can even get a thumbnail view of the accommodations at resorts you plan to visit and a listing of prices.

Almost every day provides another avenue to explore and you really don't have to be an electronic whiz-kid to operate a computer. It is a great help if you have a support group, such as the Northern Neck Computer Users, where you can ask questions on specific points, and attend special interest groups for topics you are involved in.

.NET

By Barry Simon, contributor to PC Magazine.

Microsoft's plan for the future is a vision, a plan and a mishmash. From various announcements and presentations, I believe there is a pony buried in that pile of horse manure but alas some parts of the company are so taken with the buzz around the term that everything has become a .NET even if it is distant from the true vision.

(Continued on page 4)

The Northern Neck Computer Users' Group is not a part of or representative of any manufacturer, product, reseller, dealer, consultant, or business. Information appearing in this newsletter is for the use and information of the members and friends of the group. Permission is granted to reprint any or all of the material found here by similar non-profit, non-commercial publications provided credit is given to the author of the article and "The Computer Link" is given as the source of the information. Opinions expressed are those of the authors and do not reflect those of the organization.

(Continued from page 3)

About every seven years Microsoft reinvents itself - not totally since it keeps the old stuff in place suitably evolved towards the new strategy. In 1975, Microsoft started out as a supplier of computer languages. In 1981, it took advantage of IBM's offer to become the DOS company and in the years around 1990, it morphed to the Windows company. In 1996, it embraced the web - later than some nimble newcomers but earlier than the other big guys and in an aggressive way that remade the company. I believe that we'll look back on .NET as a similar tectonic shift in the way Microsoft operates. And make no mistake: it is Microsoft's ability to reinvent itself that has caused it to thrive while the Novells and Word Perfects of the world have floundered.

While the official explanations obscure some of the key issues, I believe there are three basic concepts in play:

- centralized user data storage
- the programmable web
- a shift to software as a subscription service

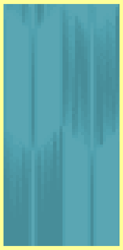
Take email - please. You access it from the office, from home and on the road. From the messages that I get as the occasional Outlook columnist for Woody's Office Watch I know that many you have problems juggling where mail is stored as you move from place to place. What we really need are ubiquitous really fast web connections and a place on the web to store our data accessible in some transparent way over the web. In some ways, this is a already there for some. For example I know people on Exchange Server at work which they then access from home and haltingly while on the road. Or there are people using Visto on the web to synch their appointments from different places. But these are ad hoc solutions for only some data. Clearly, we need infrastructure - both the availability of better remote disk services and the OS support to make their access transparent. That's the promise of centralized data storage.

With cgi, perl, VB Script, Java Script, Jave, ActiveX and Active Server Pages, you may wonder how anyone can talk about the programmable web as vision rather than reality but those languages and technologies are about programmable web pages, not the programmable web. There is still no standard for exchange of information between web sites so that, a site like Yodlee has to do its magic by ad hoc agreements with each site it scarfs data from. XML has been a work in progress now for several years and everyone agrees that it will be the plumbing below interpage programming but beyond that there is jockeying for the standard. Microsoft and IBM have embraced SOAP (Simple Object Access Protocol). Beyond ways for sites to exchange information programmatically, Microsoft's .NET programming model involves new paradigms for cross language programming.

If data is moved from local machines to the web, can programs be far behind? The third prong of Microsoft's vision is software that you run over the web. Once the software is there, the software vendor has the kind of control it can't have so easily with programs on your local machine. Some specialized software currently requires an annual license fee. There is run protection built into the product so it stops working if an annual fee is not paid but the model is regarded as heavy handed and only works in specific markets. A shift to a new model of online usage that a given user can access from anywhere could easily be accompanied by a switch to a subscription model which has long been Microsoft's dream. As programs become feature rich, upgrades become less attractive and revenue streams to vendors become less certain. The switch to subscriptions is the answer to a a software vendor's prayers. I think Microsoft may be surprised to find a reluctance of much of its customer base to be willing to make such a shift!

The first two of these elements are evolutionary in that some parts of each are present in most products that Microsoft already produces. Thus we have the absurdity that the marketing team for the latest iteration of Microsoft servers (Exchange, SQL, Commerce and 5 others) can trumpet themselves as .NET enterprise servers even though they are really very far from embracing the full .NET vision. So expect new versions of Microsoft software to have .NET added to their names whether they buy into the long term vision or not. Meanwhile, start thinking hard about how you and your company will react to a proposal for shifting to a subscription model for software for that's the one element of Microsoft's . NET vision where you and they may not see eye to eye.

(This article is brought to you by the Editorial Committee of the Association of Personal Computer Users Groups (APCUG), an international organization to which your user group belongs.)



NORTHERN NECK COMPUTER USERS GROUP
General Meeting Minutes
Saturday, April 14, 2001

The April General Meeting was called to order at 10:00 am. Al Brittle welcomed the 8 visitors and total of 40 attendees with a reminder to use the back parking lot, and be sure to visit the free table.

The Minutes of the March General Meeting were approved as published in the newsletter. The Treasurer reported total membership of 195, and placed his full report in the Minute Book.

Both computer labs are now open. In Northumberland the lab continues to be held at the Northumberland Public Library, Heathsville. In Lancaster, the Lancaster County Chamber of Commerce has made space available in its office in Chesapeake Commons Shopping Center, Kilmarnock. Both labs are open Monday thru Wednesday, 10:00 am to 12:00 noon. No decision has as yet been made by the Dupont Foundation as to the disposition of the equipment formerly used in the Lancaster Lab.

Winners of the raffle this month were Lydia Brittle (CalendarMaker software), Red Tolbert (PrintMaker software), and Lloyd Flore (PhotoShop 5.5 book).

Jim Talbot reported that the Publishing, Web Site Design and Genealogy SIGs are well attended. He asked that anyone interest in starting additional SIG on, for example, Digital Cameras, Advanced Basics, or other topics please contact him. He may be reached at www.jftmmt@rivnet.net.

Gordon Davison enlivened the meeting with a demonstration and discussion of the capacities of PhotoShop 5.5 (via its sampler), and PhotoShop LE. For comparison purposes, Gordon shared some before-and-after family photos he had clarified, repaired and/or enhanced using PhotoFinish, and the results were impressive. Thanks, Gordon!

The next Board meeting will be Friday, May 4 at 10 am, at the Northside Branch of the Bank of Lancaster in Kilmarnock. All members interested are warmly invited to attend.

Next month's General Meeting will be May 12. There being no further business, the meeting was adjourned at 11:25, with an invitation to anyone with specific questions or needs for help to stay on.

Respectfully submitted,
Camille Bennett, Secretary

Membership Report

RENEW MAY 2001- Billie Barnes, Allan Brittle, David Domas, Jean Ehlman, James Hill, Elizabeth Peterson and Rosalie Sullivan

RENEW April 2001- Julian Bell, Walter Haynie, Douglas Hundley Jr, Roland Lang, Janet Moore, Richard Newlon, Frank Pisciotta, Charles Puckett, Charlie Scott, Ray Winkel, Carol Wright and Larry Wright.

DUE FOR MARCH 2001- Stuart Bray, Garland Dillard, Linda Elders-Bailey, Madeline Kohler, Fannie Pumphey, Dick Rounds

PAST DUE FEBRUARY 2001- Norman Dobyns, Richard Orosz, Douglas Siegel.

Membership dues are $20 annually. Please send to:

John Parr, Treasurer, NNCUG, P.O. Box 10, Haynesville, Va. 22472

For insertion into our local newspaper advertising, please send to cbennett@crosslink.net no later than 15th of the month.

The Computer Link

Northern Neck Computer
Users' Group
P.O.Box 1213
Kilmarnock, Va. 22482

Special Interest Meetings

NNCUG GENERAL MEETING
2nd Saturday 10:00 a.m.
Lancaster Community Library

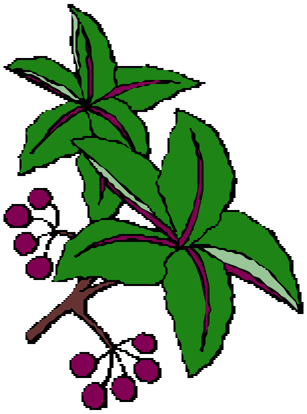
WEBSITE DESIGN SIG
info (804) 462-7898

INVESTMENT SIG
(discontinued)

GENEALOGY SIG
June 11, 2:30 P.M.
Lancaster Library.

PUBLISHING SIG
May 10, 2:00 P.M.
call 435-2011
for location

For just $5 per month
your advertising can appear
here



Coming Attractions

May 12........Mike Erskins talks about Security
June 9........Executive Software Presentation.....DEFRAG!