



**ATTORNEY JANET RENO'S WEEKLY MEDIA AVAILABILITY**

**WITH MICHAEL VATIS, NATIONAL INFRASTRUCTURE**

**PROTECTION CENTER TO DISCUSS NEW E-MAIL VIRUS**

**JUSTICE DEPARTMENT, WASHINGTON, D.C.**

**MAY 19, 2000**

**9:33 A.M. EDT FRIDAY**

ATTY GEN. RENO: The FBI has opened an investigation into a new, more destructive variant of the "love letter" worm.

This new worm is NewLove.vbs, which was identified yesterday. Like the earlier versions, this worm is transmitted via e-mail, but unlike the others, this new version can change the subject line and the program code every time it is retransmitted. This makes the virus more difficult for users and anti-virus programs to detect. The worm is transmitted when a user opens an e-mail attachment.

The NewLove.vbs virus uses the file name of a file that a user has recently been working on, and places that file name in the subject line of the e-mail transmission. The recipient may think that they have been forwarded a file from a known associate.

When the attachment is opened, this worm can damage all files not currently in use by changing the file extensions to .vbs. It can also transmit itself to a new group of victims taken from the current victim's e-mail address book. The new e-mail will have a different subject line, taken from a file name that the current victim has been

recently working on.

If you receive an e-mail with a .vbs file extension, do not open it, even if it comes from a trusted source. Delete the e-mail from your system.

Michael Vatis from the National Infrastructure Protection Center is here with me to answer any questions you may have.

Q Mr. Vatis, from the sound of it, if it uses a vbs extension, I gather that it uses Microsoft Outlook to --

MR. VATIS: Correct.

Q Then how do you -- do you usually see file extensions, would you usually see extensions in the file name in Microsoft Outlook? How would you know whether you had an e-mail with that extension?

MR. VATIS: Our understanding so far of this is that the name of the document that is being transmitted that will contain the virus will be in the subject line of the e-mail, but that subject line will not contain the dot-vbs extension. However, in the body of the e-mail you will see the dot-vbs, so if the e-mail is opened you will be able to see the dot-vbs, which will indicate that this is probably an infected file and you should not open the attachment to the e-mail.

Q So it's opening the attachment that would spread the virus into your computer?

MR. VATIS: Exactly.

Q How widespread is this thing? It seems like "I love you" was all over the place before people knew it. This seems a little slower to go global.

MR. VATIS: We don't know yet exactly how widespread this is. In the early morning hours of today we did have reports of upward of 1,000 machines being infected. I suspect it's

somewhat larger than that now, but we don't have any final fix on how widespread it is. Unlike the original love letter virus, this one appears to have started, at least in significant part, in the United States, rather than spreading from Asia to Europe to the United States.

Q And the patch that Microsoft is offering, will it protect a system against the new variant?

MR. VATIS: We haven't yet evaluated the various patches that are available, but we do know that the major anti-virus vendors are working on detection software for this variant. But people should check with their anti-virus vendor to see whether they've got an update yet to their normal anti-virus software.

Q Do think you're jumping on this more quickly than you were able to on the love bug?

MR. VATIS: We jump on all these as quickly as we can. It's important, when we first get a report in, that we assess the information, that we check with other sources to see if this is a significant virus, to see if fixes are available, so that when we do go out with notification to other agencies, to the public, that we have as much information and that we've assessed and determined that it's credible before we go out. So in this instance, we started notifying other agencies at approximately 2:00 a.m. this morning and have been issuing further alerts through various mechanisms to the public, to private industry and to federal agencies by various means. But that started around 2:00 a.m.

Q When did you get your first reports of it?

MR. VATIS: Just slightly before that.

Q Michael, is there any particular section of the country more affected than others?

MR. VATIS: It's too early to say at this time, but we have seen reports of infection across the country.

Q The Love Bug worm would send copies of itself to all of the addresses in your Microsoft address book. Does this thing do the same? How does it transmit itself to others?

MR. VATIS: From what we know so far, it propagates in the same manner; that is, by sending an e-mail to, we believe, all of the addressees in your e-mail address book. What makes this somewhat more dangerous, as the attorney general said in her opening remarks, is that it doesn't send an e-mail with a subject line that everybody can look out for, that says, "I love you," or something else. This one takes the name of an actual file in the infected user's computer -- so it appears to be a legitimate file -- and then sends that. And this is known as a polymorphic virus or worm in that each time it's transmitted, it comes in a different guise so that -- that's why we have to alert people not to open any e-mail attachment that comes, where the document in the subject line has a ".vbs" extension because we don't know -- it varies in each instance what the actual document name will be.

So people need to be much more vigilant in looking at e-mails.

And again, just as with the original love-letter virus, the e-mail will appear to come from someone you know, and it will actually come from that person's computer. It just will not have actually been sent by that individual pressing "transmit." The virus will have sent itself.

Q Because of that, would you say that this one is more complicated, the code is more elaborate, than the last one?

MR. VATIS: Our initial assessment is that this is more complex. As is typically the case with viruses, you see an evolution, and this is the latest stage in the evolutionary process from the love-letter virus. So essentially, it propagates itself in the same way, but it disguises itself in a more sophisticated fashion. So that is potentially more dangerous. It also has a greater capability to erase files on a system. At least at this point in time, that's what it seems to be capable of doing.

Q When you talk about the "evolution," does that mean that it grew from -- you know, it's -- first, there was the Love Bug -- this is the next generation; it's almost like another version of a copycat?

MR. VATIS: Yes, precisely. It evolves, not in the biological sense, but in the sense that people take the code from the initial variant and then change it in ways that try to evade the anti-virus software that's been put out for the initial variant. And that also tries to trick users who now are vigilant to the possibility of receiving an infected e-mail. It tries to still trick them by disguising itself in different ways. So in that sense it is more complex.

Q What do you suspect about its origins, where it may have come from?

MR. VATIS: I can't say at this time. We are investigating to determine what the source might have been.

Q But you do think it's a copy-cat, not the same source as the original?

MR. VATIS: I can't say at this time. But we are looking into all possibilities.

Q Is it more difficult to track for the reason you just stated?

MR. VATIS: At this time I can't get into the investigative strategy or process, but we are looking at all possible leads, as we do in these cases.

Q How much has government been affected by this? Can you say that?

MR. VATIS: We don't have any firm fixes yet. Obviously, the warnings were all disseminated before the start of business today. Hopefully, that will minimize the effects within the federal government community and across the private sector as well. But it's too early to say yet what the impact has

been or will be.

Q Mr. Vatis, does this worm go after any specific files, or just any file it gets its hands on?

MR. VATIS: It appears to go after most files in a computer other than those in the root directory. That's our understanding from the anti-virus vendors so far.

Q Can it destroy these files?

MR. VATIS: It basically reduces them to zero, so yes, it erases the files.

Q Everything on the hard drive is erased.

MR. VATIS: Most files, other than those in the root directory, are potentially subject to being erased. That's our understanding so far.

Q It doesn't just change the name?

MR. VATIS: It adds a .vbs extension to the files and then reduces their content to zero. So it effectively erases them. But again, this is all based on our preliminary analysis overnight so far, so our understanding may change as we examine this virus further.

Q What about deterrence? There were some indications, some reversals in the Philippines, that these weren't being considered serious crimes. Is there any thought, either Ms. Reno or Mike, is there any thought to filing U.S. charges against any suspects in the Philippines or against any suspects who are discovered in this latest -- (off mike)?

ATTY GEN. RENO: I think while the investigation is pending, we really shouldn't comment. We're working with the Philippine authorities in a good, close working relationship, and I think it's important that we continue that effort.

Q But how do you stop these types of attack unless you have

some very high-profile prosecutions and some rather long prison terms handed out at the end of it?

ATTY. GEN. RENO: We don't comment on what's going to happen in an investigation, as you well know, because we're going to do it based on all the evidence and what's best for the case.

Q Mr. Vatis, it looks like it's become a plague of viruses; I mean, from the Love Bug to the copycat viruses to this polymorphic virus. I mean, every single place you turn, there's another virus. How are -- I mean, does that mean you're overstretched right now in terms of dealing with -- You're obviously not putting the Love Bug investigation on hold so you can deal with this one, but you only have a set number of people.

MR. VATIS: We are seeing an increase in the number of viruses and also in the sophistication of the viruses, which means that there are possibly greater impacts and of course more criminal investigations. As we've said in congressional testimony and publicly several times, computer crime in general is on the rise and we are taking all possible steps to make sure that law enforcement in general is well-situated to deal with this new set of criminal activity.

ATTY. GEN. RENO: I think one of the points that has got to be made, though, is that it is critically important that law enforcement and the industry work together, with industry taking the lead in developing programs that prevent this. What's happened is exciting, but it also presents us with an extraordinary challenge. Great minds have been putting together something that would permit us to communicate as we've never communicated before, but as we developed the technology, I don't think prevention mechanisms that ensured privacy kept track. And so it is important for us all to develop the prevention programs, and I think industry is better suited to do that, and for us to work with industry in terms of pursuing criminal investigations.

One of the things that I've learned is that if you've got a balanced program of prevention and punishment, no matter what it is, you're going to be more effective.

Michael, is that --

MR. VATIS: Yes, I think that's a critical point. Criminal investigation is an important element of deterring these sorts of criminal activities. Issuing warnings as quickly as possible is also an element of prevention, but I think the main focus has to be on the part of industry to develop technologies that prevent people from being subject to malicious viruses in the first place.

And that's really where I think we need to put our main focus because no amount of warning will ever eliminate the damage that can be caused by a virus, as long as systems can be so easily affected by these things.

Q Do you ever put any numbers on the increase in the number of virus attacks?

MR. VATIS: I don't have any at my fingertips right now. But we have seen a steady increase in destructive viruses.

Q Will you do that later?

MR. VATIS: Sure.

Q We hear about these dramatic viruses. But roughly speaking, how many new viruses do you all encounter every week?

MR. VATIS: The anti-virus community in the private sector sees in the hundreds of viruses any given week. We have seen estimates that there are 20 or 30 new viruses a day. Not all of those have the sort of widespread and destructive impact as the Melissa virus or the Love Letter virus or the most recent virus. And that's frankly why it's necessary to assess the spread and the destructive potential of a virus before we leap into action by issuing warnings and doing other things, because not every virus



really makes it out into the wild in any significant way. But there are literally thousands -- many thousands of new viruses a year. And I think right now there are over 50,000 viruses that are known to be out there in the wild to some degree.

Q Mr. Vatis, the Love Letter worm had an apparent purpose, which was to try to detect passwords and send them back to an Internet site. Does this one have any other apparent purpose, other than just sucking the brains out of your computer?

(Laughter.) Just -- does it appear to do anything for the person who started it?

MR. VATIS: Based on the analysis that we have done so far, and that the anti-virus companies have done so far, the things that this virus does are: number one, to propagate itself by sending e-mails to people in your address book; and number two, to erase files. We have not yet seen whether it has the ability to snatch passwords and send those out, but that's one of the things we are looking at.

Q Mike, the so-called hackers were, I believe, of tremendous use in the DDOS investigation. They really helped the bureau.

MR. VATIS: I can't comment on that at this point since it's still a pending investigation.

Q Any thought to building some kind of a Neighborhood Watch, on the Internet community -- (chuckles) -- with a posse in the Wild West of the Internet to help?

MR. VATIS: As the attorney general said earlier, cooperation by the private sector with us is critical in all aspects, in prevention and also in the pursuit of investigations.

We don't encourage people to engage in any sort of vigilantism on line or creating posses that might potentially violate the law in their own activities if they

begin hacking into people's systems to find information. So we are always encouraging people to come to us with any information that they might have. We also seek out expertise in the private sector. But we strongly discourage anyone from pursuing self-help remedies that could potentially violate the law.

Q Are there any particular systems that are more vulnerable than others? For example, it seems like Microsoft Outlook is constantly under attack here and being used. Is that more vulnerable than, say, Lotus Notes or some of these other products out there?

MR. VATIS: I don't want to comment on the relative vulnerabilities of systems. We do see Microsoft being affected with greater frequency, but that is at least in significant part because Microsoft has probably the greatest share and the greatest number of users out there. But I can't comment on the relative vulnerability of particular products.

Q How much, if any, evidence do you see that any of these orchestrated, organized attacks or perhaps probes to identify points of weakness for some larger assault later on?

MR. VATIS: As a general matter, we do see in many of these cases, whether they involve illegal intrusions into systems or the propagation of viruses, we do see some organization, often online organizations, people getting together in Internet relay chat sessions or through e-mail groups. That's really the most I can say on that right now.

Q You don't see evidence of organized criminal activity or state-sponsored activity?

MR. VATIS: As a general matter, the spectrum of threats online does include organized criminal groups engaging in hacking or online extortion or things like that, and we've had cases that involve that sort of threat. And the threat from foreign nation states is also one that we are very mindful of and are constantly trying to gather information

about potential threats.

Q New reports about an old story, in some ways, a Freeh memo raising concerns about alleged comments, I should say, by Lee Radek, the head of Public Integrity.

What do we draw from that? And was there any pressure on Mr. Radek not to go forward?

ATTY GEN. RENO: Well, I think Mr. Radek should speak for himself, and he happens to be in Prague. But I am --

Myron spoke to him last night, and he said, "I have no recollection of ever saying, 'I was under pressure because the attorney general's job hung in the balance,' nor is it something I would have said, because it has no basis in fact."

As for me, I call it like I see it, regardless of the consequences. I have got a month-to-month lease on my apartment, and I have been prepared to go home from the beginning. I have tried to make clear to everybody in the department that they should do the same thing and call it like they see it.

Q Ms. Reno, do you have a recollection of the discussion with Director Freeh in which he referenced these purported comments from Mr. Radek?

ATTY GEN. RENO: I don't have a recollection of him stating it and talking about pressure because of the job. I do have a recollection of him saying that we should get a junk-yard dog to prosecute the case, but I think that was said on several occasions.

Q Do you recall his saying anything about Mr. Radek and why Mr. Radek should be replaced or why Mr. Radek should recuse himself?

ATTY GEN. RENO: He had some discussions about Public Integrity on a continuing basis. And he talked about getting a -- what he referred to as a "junk yard dog."

Q Just going back to Mr. Esposito's version of this or last version of this, he is very senior former FBI official. Does it trouble you that there is this discrepancy between what he remembers and what Mr. Radek remembers?

ATTY GEN. RENO: I think you should check with Mr. Esposito as to what he remembers.

Q Ms. Reno, the Congress has subpoenaed or asked for, documents several times on the campaign finance investigation.

Do you have any idea why this memo is just coming out now?

ATTY GEN. RENO: No, I don't.

Q Ms. Reno, on the Columbia settlement, the company kind of spilled the beans yesterday. Can you confirm the general outline that was in the story that the company released?

ATTY GEN. RENO: I think we can. But for several years the department has been investigating allegations of fraudulent conduct by Columbia HCA Health Care Corporation in connection with the operation of its hospitals and other facilities.

During this time period, we have had discussions with the company about resolving its civil liability for these allegations.

The department has reached a tentative agreement with Columbia -- tentative, I point out -- which, if formally approved by the department, would resolve a number of issues under investigation.

The agreement would resolve, in part, Columbia's civil liability to the United States, but would be conditioned on a number of future events. Any formal agreement must be authorized by appropriate department officials in consultation with other agencies. We have no further comment on the ongoing discussions.

Q Ms. Reno, the National Rifle Association is beginning its annual convention this weekend and claims to have gained significant numbers of new members in the past year, as the gun control debate again comes to the fore. What's your sense of where the political dynamic is after the Million Mom March? Do you think there is a change here in public interest in gun control?

ATTY. GEN. RENO: I don't see how you could listen to those marchers, listen to what went on and, not from politics, but from simple common sense and from regard for human life, not feel the impact of them.

Q What will the lasting impact be, though? It was a very emotional weekend. Do you get the sense that that can be translated into political action?

ATTY. GEN. RENO: I get the sense that those organizers and the people who participated and others who cheered them on are absolutely determined, and they are not going to give up.

I remember when we first started out focusing on drunk driving cases. We did not have a MADD, or Mothers Against Drunk Driving, chapter in our jurisdiction. I happened to be in another jurisdiction where they did, and those mothers were so vociferous and outspoken and tenacious, I thought, "Wouldn't it be wonderful if we could get them established in Dade County?" They did, and sometimes it was a slow process, and sometimes they would come to me saying, "Are we having any impact?" And then they began to see their impact, and I think we will feel, not from political reasons, but because it's right.

Q Ms. Reno, have you been briefed on the internal -- your internal review of the Wen Ho Lee case? Have you been briefed on that, or will you be sharing the report with the Congress?

ATTY. GEN. RENO: I have been briefed on it, and I am in the process of reading it. It has something like 790 pages or something like that, and a number of appendices. The work

that has gone into it is just extraordinary.

It is detailed, it is comprehensive, it is thoughtful, and I just appreciate the efforts that have been underway.

I also appreciate the fact that the Bureau, the Federal Bureau of Investigation, has been very forthcoming and cooperated, and I think we're all interested in using the contents of this report to shape the future efforts in this regard.

I very much would like to share it with Congress, and we are looking at that from the point of view of how we can do it, hat we can share, consistent with pending matters and any other consideration that might be involved.

Q What are the most important lessons that you take from this study?

ATTY. GEN. RENO: As I indicated, I want to read the report myself and absorb all the facts before I comment.

Q Ms. Reno, President Clinton has confirmed that bin Laden was the leader behind the bombing plot attempts during the 2000 rollover, especially the one that tried to come through into Washington state. Can you add anything more to the -- especially the link to bin Laden? Can you amplify what the president has said?

ATTY. GEN. RENO: No, I can't comment.

Q And just this one more thing, there is -- there were two other threats mentioned in the articles. Do you need more money than is being asked for? Are you concerned about miniaturization of weapons, especially nuclear weapons? And are you concerned that there will be a power play and chaos will reign when Mr. bin Laden dies?

ATTY. GEN. RENO: You want to start with just one?  
(Laughter.)

Q Let's start with miniaturization.

Q With chaos reigning! (Laughter.)

Q Miniaturization; was that something that's --

ATTY. GEN. RENO: Would you define --

Q Miniaturization.

ATTY. GEN. RENO: Yes. Would you define it? I hear it in so many different contexts, I think it might --

Q The worry about weapons of mass destruction being miniaturized and then easily smuggled and easily carried to sites of terrorist attack.

ATTY. GEN. RENO: I think that is a concern that must be addressed.

Q And Mr. Laden, are you concerned that his bad health could lead to a power struggle within the terrorist organizations?

ATTY GEN. RENO: I have no comment about his situation, but I will say that it is incumbent upon us all to pursue every inquiry to make sure that we protect the national security of this country.

Q Ms. Reno, given the president's bully pulpit, is there any concern that his comments about bin Laden could affect the pending cases?

ATTY GEN. RENO: I simply don't think I should comment.

Q Do you have any observations about the meeting on Mexican drug cooperation yesterday? You were over there, weren't you, at the State Department?

ATTY GEN. RENO: Yes. I think we had a good day.

Q Mike, is that a computer virus on your tie? (Laughter.)

MR. VATIS: Every day for an Irishman is St. Patrick's Day.  
(Laughter.)

Q Does the virus have a special name, or just the NewLove bug?

MR. VATIS: At least some of the anti-virus vendors are calling it VBS.NewLove.A.

Q (Off mike.)

MR. VATIS: I think for shorthand, NewLove. Other people are also calling it Herbie. (Laughter.)

ATTY GEN. RENO: With that, thank you.

Q Thank you very much.

END.