

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE  
(PUBLIC AFFAIRS)

4 November 1988

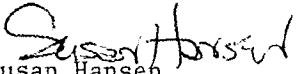
MEMO FOR Secretary Carlucci

Sir:

In conjunction with the attached transcript, we have been advised by Col Cole of your staff of the following information:

Mr. Richard Gronet, Director of Policy, NSA, has been given to understand that John Markoff, a reporter for the New York Times, will run a story tomorrow stating that the perpetrator of the computer virus is the *son* of a current employee of the National Computer Security Center at Ft. Meade.

We have no confirmation of the identity of the individual.

  
Susan Hansen  
Defense News Division  
OASD (PA)

INFO VIA TELECON FROM NSA



1988

News Briefing by

Dr. Raymond S. Colladay, Director  
Defense Advance Research Projects Agency

Col. Thomas M. Herrick, USA  
Deputy Director, DCA Data Program Systems  
and Program Manager, Defense Data Network

At the Pentagon

Friday, November 11, 1988 - 5:00 P.M. (EST)

Mr. Fred S. Hoffman, PDASD/Public Affairs: Good afternoon. We brought down two of our experts to discuss with you the scope of the computer virus that you are all interest in. Dr. Raymond S. Colladay, is Director of the Defense Advanced Projects Agency, and with him is Col. Tan Herrick, Deputy Director of the Defense Communication's Agency Data Program Systems and Program Manager of the Defense Data Network. Dr. Colladay will have a brief opening statement and then take your questions, Dr. Colladay.

Dr. Colladay: We first detected a virus in the system of the network late Wednesday afternoon, actually it was about 6 o'clock, Pacific Time, on Wednesday afternoon, and immediately threw into action the experts that went to work to try and isolate and fence off this particular virus. That was successful. The virus was identified. The program was debugged and the trap doors were identified that would separate it off and then immunize the rest of the system.

It came in through a debugging feature on the electronic mail, by a user. It did not affect the protocol or the operating system of the ARPA net. Once that that was identified we could easily find a fix for it. That was communicated to all the users on the network. At this time, we feel confident that the problem has been solved; that the program that caused the problem has been isolated and that the system, the network is immune to any further problem.

It was a benign virus, by that I mean it didn't destroy files. What it did when it got into the system is add files and saturate the memory. So it was easily identified. But it has been dealt with effectively and eliminated from the system.

Q: Could it just as easily been a malignant virus that could have destroyed existing programs?

A: That is always a problem and a threat. We moved quickly enough to isolate it. Even had it been a malignant, more damaging virus, we would have caught it quickly, but yes. That is a possibility. In this case it wasn't.

Q: How many computers and what installations were affected by this?

Q: Name some Defense Department installations that had lost their access, their computers on these nets.

A: These were primarily research users. It was identified at MIT and University of California, Berkeley, Stanford, in our own computers at DARPA, and it was isolated in that community.

Q: Can you give us a rough number of how many computers you're talking about?

A: There were several dozen installations that were affected.

MORE

413.51

11 NOV 88

Q: Several dozen installations out of a network of what?

A: A network of *some 300*.

Q: All defense, you're talking?

A: No, these were university users and part of the R&D community.

Q: There was no classified information?

A: No classified information.

Q: Does this indicate a potential vulnerability in your Defense computer network? Could such a **virus** be planted in systems that have a network that relate to classified information?

A: We believe we have sufficient safeguards in tagging users in the classified system that that would not be affected on this. We can implement those kinds of similar systems in the ARPA net and it's a matter of cost. *By similar systems I mean taking the more effort to tag the users so that they are identified.*

Q: Could this particular **virus** have passed from the network in which it was found into other networks, I think particularly of the WINEX and other national security networks?

A: Let me defer the answer to that question to Colonel Herrick who managed the gateway between these different networks.

A: To answer your question, absolutely not. They are separate networks and they are separate for the reason of security. *So there is not a linkage between an unclassified network and a classified network.*

Q: It could not have gotten into NORAD or into SAC or into WINEX?

A: Not in the scenario that you're describing, absolutely not.

Q: From this particular network it wouldn't affect it.

A: No.

Q: What if a user using a terminal went from this research network, **who** was also cleared to use say a WINEX terminal or any of the others. Could there be any overlay under those circumstances?

A: No, because they're separate networks. *What you have to understand is that one of the safeguards is that WINEX, the -- computer network, for instance, is a closed community and on it are only members of that community. They are unable to have access from outside of that community so you cannot get on a terminal outside of that community and enter the WINEX computer network. You have to be in the network, you have to be cleared, you have to be a registered individual within the network.*

Q: I'd like to ask you if you have an effort underway as to "who done it" and who is investigating the possibility of finding out who did it, and is there anything you have to do, you said the damage was contained other than isolating the virus and the time that took. Does anything have to be done differently from now on in your own system to keep this **from** occurring again?

Q: And also, do you have any idea where it might have originated?

A: We don't know yet the source of the **virus**. We are in the process of analyzing that. It's very complex in marching back through the network tree to the source. We're still analyzing that.

MORE

As far as lessons learned, we understand the vulnerability. We have, in the case of the research network, elected to not implement all of the protective features that one could in terms of tagging messages in the electronic mail system. We will be revisiting that and trying to decide at this point whether more protective features need to be added to the ARPA net system.

Q: Is that your investigation you just mentioned, or someone else's?

A: We're looking at it in DARPA. I started a study today. As soon as we isolated and found the problem we went into the mode of doing an analysis of what happened and lessons learned. I don't think we will be the only ones to do that, but I started it in DARPA today.

Q: When did you find the bug, and did you ever shut down?

A: Yes, we went off the line immediately. That was the first thing we did, as did the other users. We found it --

Q: The net went off the line or DARPA went off the line?

A: DARPA went off the line. See, the problem wasn't with the network, it was with the canputers on the network. So the first thing to do is disconnect from the network. We did that. The experts around the country at Stanford and MIT and Berkeley and DARPA and elsewhere immediately were in contact with each other working on the fix. It was isolated and the program was actually downloaded, the program that was the problem, the parasite on this debugging routine, was identified. So we knew precisely what the program was. Therefore, we knew precisely &at the fix was. As soon as we had put that fix in place we could get back on the line. We did that today. We've been on the line all day today as have the other users because of the confidence that we found the problem and fixed it.

Q: So you were down for a day then.

Q: You said you had not found the source. Do you know whether it came from MIT, &ether it came fran, you don't know the programmer, but have you narrowed it down to an area of the country?

A: No we haven't. We have not yet narrowed it dawn to even a particular location.

Q: What's the likelihood that you will?

A: I think it's fairly likely that we will be able to identify the location, but I think it would be very difficult to in turn find the individual perpetrator.

Q: Did you say that all canputers on this net are now back up and operating?

A: We have no way of knowing for sure, but everybody that we have been in contact with that are on the net are back up on the systan.

Q: We've been talking about computer systans sort of at the two extremes, this unclassified data sharing network, and then NORAD type computers for control of forces. What about all the canputers in between? The computers that keep track of pay records, spare parts, etcetera, etcetera. Could they have been vulnerable to a slop-over fran this particular virus? Or would they be vulnerable to an episode like this where either a prankster or a disgruntled employee would get on the net and screw it up?

MORE

A: They are, as Colonel Herrick said, they are separate networks that are linked by gateways. Those are control points. But I'll defer to him for a further answer to that question.

A: In reference to whether or not another computer or another system could have been compromised or penetrated in this situation, we do not believe so. The reason is if you go back and look at specific, we have the code so we know what the code was trying to do. If you take a look at what the code was trying to do, it wasn't designed to do anything more than be a nuisance. So the specific answer to your question is no.

The larger answer to your question is when you deal in areas such as pay or logistics, you also have methods within that to make sure that those records are accurate, so there are internal checks.

Q: I'd like to go back to an answer you gave to a previous question and make sure I understand you. Computer experts have been telling me today that this shows how quickly and how massively a system can be affected and how vulnerable a system is. Do I hear you correctly in saying you are aware of how vulnerable the system is?

A: We have been concerned about this and have been aware of the vulnerability and have taken safeguards within reasonable cost of dealing with it. Now that question comes in of reasonable cost. You can never, I don't believe, reduce the probability of this happening to zero. But there are further things that we can do to prevent it in the future. More interrogation, more tagging of users, but they are certainly possible, and in the more secure systems we do that, and we're going to be weighing the costs against the advantages of further security in the system. But yes, there's no question that we are vulnerable to these kinds of virus attacks.

Q: You said earlier that you had elected not to implement all of the potential safeguards that you knew were available. Can you tell me some of the reasons that you elected not to implement all of the safeguards?

A: As I just said, it's a cost trade.

Q: You suggested that the method of tagging users was part of what made the various classified networks that the Pentagon uses less vulnerable to this sort of thing. What happens if a determined user is perfectly willing to allow himself to be identified and is disgruntled or whatever, almost a suicide attack if you will? Can it happen?

A: You have to get into what's the probability of that happening. We think we've safeguarded against that to any reasonable probability. But that's not zero. We recognize that vulnerability and we deal with it in matters of security and we think we have done that.

Q: I take it that you think this was a prank that was done deliberately rather than it was an accident or somebody making a mistake on a terminal. From what you've seen so far, can you enlighten us on that?

A: I don't believe it was an accident. I think it was deliberate. Whether it was a prank or whether it was someone that wanted to dramatize just how effective propagation of a virus like this could be, I don't know. But I don't think it was an accident.

MORE

Q: Do you see any need for criminal sanctions in this area, both as a deterrent and also to bring in investigative agencies when something like this happens that could aid your task in finding the perpetrator?

A: I can't really answer that. I think it's something that we should address, but I can't *from* the standpoint of a DARPA Director, I can't really address that.

Q: Would you go **back** to the beginning and be a little more explicit as to what you exactly saw? What was the phenomenon that you observed, and where was **it**?

A: What we saw, and it occurred not in an isolated location. It was in several locations. I think **it was** first found at UC Berkeley. The system was generating files. It **was** not destroying anything, but files were being created, if you will junk mail.

Q: Was **it** replicating itself?

A: It **was** just generating files that **were** not **part** of the system. That's pretty easily detected. Then the computers were immediately taken off line.

Q: Was **it** printing out?

A: No, you don't have to print them out in hard copy, but you see the files generated, and you see memory vanishing.

Q: This **was** late Wednesday?

A: Late Wednesday.

Q: How **long** were the computers off line?

A: **We** were starting to get back on line late yesterday so I don't know exactly, but I think **it was** around 24 hours we had **it** isolated **and** fixed.

Q: From **what** you know of this **virus**, how long would **it** have taken to do this program, and what level of computer **savvy** was necessary to **come up with** this?

A: I really can't answer that. I don't know. It wasn't a neophyte. It **was somebody** who understood the system well enough, was sophisticated *enough* to be able to tie back to this de-bugging routine on the electronic mail system and know that would get propagated.

Q: Are there thousands of grad students who could do this, or just a handful of people with that knowledge?

A: I don't **know**. I couldn't answer that.

Q: Should **we** add computer terrorism to our vocabulary? How do **we** protect smart weapons?

A: **As** we've said, there are ways of protecting it if you're willing to pay the cost of doing that as security requirements are higher. In this case we felt **it was** a reasonable trade. Computer terrorism, I think we're living in an age where we're vulnerable to this kind of thing and that's not a bad term to describe **it**.

Q: How serious do you consider this? We've had this before, I believe, with hackers getting into the Pentagon systems and playing with **them**. **Is** this the first time we've had this **type** virus in a Pentagon system or a research system? How serious do you place this among these occurrences?

MORE

6.  
A: This is the first time we've had something like this in the network, but again, let me say that it's not endemic to the network. It came in through a user. SO it wasn't a fault with the network. It was on a user program.

I can tell you ~~from~~ my standpoint that I take it seriously. DARPA has pioneered a lot of the computer network system and ARPA Net that has led to other networks and we're *moving* on in our research to *more* sophisticated systems, and network security is going to be *part* of the research program. We take it seriously.

Q: Can I just ask you to *sum* up, no damage was done at *all* except for the frustration and time lost? *Or* was there some real damage. If I asked the question what was the specific damage done here, how would you respond to that?

A: The damage was lost time. here was no damage that we know of to any files or destruction of any files.

Q: What do you think it cost in terms of time lost and the effort that it took to clean up the mess?

A: I don't know, because we're not done yet. We're still going through the post-analysis and we are still trying to track back to the source. I don't know what it will be.

Q: In the past breaches of computer security, and instances of hackers breaking into things, the FBI has confiscated computer systems and has in fact arrested and provided witnesses and so forth against other hackers. Is the FBI involved in investigating this particular breach? This particular virus? Are they investigating along with DCI or.. .

A: We have been in contact with them. We have been preoccupied with identifying the fix and not so much on the investigation, but we've been in contact with them.

Q: But there is an investigation underway that you know of? Is there a joint DoD/Justice Department investigation?

A: I don't know that. I meant an analysis from DARPA in trying to isolate what happened and understand what happened.

Q: The letter writer to the Times or the telephone caller, suggested that this got out of hand. From what you've seen of the program that's in there, is this something that could have gotten far beyond what the prankster intended?

A: I don't know what the prankster intended, or whether it was in act a prankster. I don't know how to answer that. I can't say I don't believe it did get out of hand because we were able to isolate it and eliminate it quickly.

Q: Was it beyond what he intended though? Could you tell from the nature of the program?

A: I don't know what he intended.

Q: Do I understand you to say that as a result of this incident DARPA is redoing its look at computer security, or is that an ongoing concern? And second, has this incident caused the Pentagon security people, and computer

MORE

security people generally to look at all of their other systems as well?

A: Any time you have an event like this it heightens awareness and sensitivity. It's already, I believe high. What I said before was that the DARPA computer network research program is going to take an even more active role in focusing on network security as well.

Q: Are the SAC and NORAD systems closed communities as you described, as well as...

A: To the best of my knowledge. The network that I run does not include SAC and NORAD.

Q: If on one end of the extreme a system that I can get into every day with my home computer is an open system, and the system you describe as a closed community system, where does this computer network fit in between? Is it terribly open? Is it terribly closed?

A: If you deal in an area of research and development where you're dealing with colleges and universities and people where you want to take information and broadcast it, then you have a very open system. It was designed, and has been designed to be that way.

Q: You said it was a tradeoff, cost for security. How much would a system cost that would have prevented this?

A: Until we finish the analysis of &at it would take, I can't put a price tag on that.

Q: How many users are in this network? How many computers or users were shut down? Do we have any number?

A: I recall a number on the order of 300. That's the order of magnitude.

Q: These are research institutions all across the United States?

A: That's right.

Q: I'm not as familiar with the story as I should be, but this is the only research network that was shut down. There weren't others that were shut down also?

A: That's correct.

Q: Again, I just sort of want to understand the chronology a bit. When you're saying it was discovered at University of California at Berkeley and there are 300 institutions that were shut off, how did that happen? Did Berkeley call Washington and say we've got a problem, cut your computer off? How did the news spread?

A: By telephone and by the computer network itself. Remember, these people are in contact, they're colleagues so they're in contact regularly anyway.

Q: If it was discovered at 6:00 o'clock Pacific time, how long before all these 300 knew about it? How long before people were getting off?

A: I can't answer that. I know we came off immediately and I suspect most people did, but I can't put a time frame into it.

Q: Is there any indication the perpetrator inserted any Trojan Horses full of viral infections that will come out like a time bomb later on? Could you isolate that out? And also, did this spread internationally at all?

MORE



A: No, it didn't propagate internationally that we know of. And while there is always a possibility for some latent bug to wreak havoc, we're as certain as we can be that that didn't happen in this case because we were able to extract the actual program that did the damage and we understand that program well enough to be able to write an antidote for it. So we're pretty confident that that didn't happen.

END

**NATIONAL  
SECURITY  
ARCHIVE**

This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, [nsarchiv@gwu.edu](mailto:nsarchiv@gwu.edu)