

VIRUS INVESTIGATION FACT SHEET

(Fax Attn: Andrew Cooke 301-903-2451)

INVESTIGATION FORMS MUST BE RETURNED TO VIRUS COORDINATOR WITHIN 1 DAY OF RESPONSE.

SECTION 1: GENERAL INFORMATION (All Incidents)

Applix #:	Date:	User:	Org.:
ViRT Member:		Arrival Time:	Departure Time:

ANTI-VIRUS SOFTWARE

<p>On-site symptoms (circle one):</p> <p>Monitor detected SMTP Gateway notification</p> <p>Scanner detected Post Office notification</p> <p>System behavior Server notification</p> <p>MS Office alert E-mail notification</p> <p>Other: _____</p> <p>_____</p> <p>_____</p>	<p>Is anti-virus software installed? Yes No</p> <p>Package: _____ Version: _____</p> <p>Signature file date: _____</p> <p>If NO, did you install? Yes No</p> <p>If outdated, did you update? Yes No</p> <p>Software used for eradication (circle one):</p> <p style="text-align: center;">McAfee Norman Norton Trend Micro</p> <p>Other or tool: _____</p>
--	--

VIRUS INFORMATION

<p>Virus Name: _____ (If more than one virus found, create separate incidents for each.)</p> <p>Virus Type (refer to VirusBase for confirmation):</p> <p>Boot Sector Virus: _____ (Fill out Section 4)</p> <p>Macro Virus: _____ (Fill out Sections 2 & 3)</p> <p>Application Infector: _____ (Fill out Section 3)</p> <p>Trojan Horse: _____ (Fill out Section 3)</p> <p>Start-up Executable: _____ (Fill out Section 3)</p> <p>The virus was received via:</p> <p>E-Mail: _____ (Fill out Section 5)</p> <p>Diskette/other media: _____ (Fill out Section 6)</p> <p>Shared Resource: _____ (Fill out Section 7)</p> <p>Internet: _____ (Fill out Section 8)</p> <p>IP/Network: _____ (Fill out Section 9)</p> <p>Other: _____ (Provide details in Sect. 10 Notes)</p>	<p style="text-align: center;">Refer to the VirusBase listing at www.microtech.doe.gov/v_index.html to answer the following questions.</p> <p>Is the virus a known DOE virus (is it in VirusBase)? Yes No</p> <p style="text-align: center;">(If NO, page the ASSIST immediately at (202) 539-3808. Obtain copy of diskette (boot sector) or file (other).)</p> <p>Is the virus destructive ? No Minor Medium+</p> <p>Is the virus network-aware? No Minor Medium+</p> <p>Can the virus cause data compromise? No Minor Medium+</p> <p style="text-align: center;">(If Medium+ for any answer, page the ASSIST immediately at (202) 539-3808.)</p> <p>Has the virus infected a server or other shared resource? Yes No</p> <p style="text-align: center;">(If YES, page the ASSIST immediately at (202) 539-3808.)</p>
---	--

SYSTEM INFORMATION

System Tag #:	OS:	IP Address (run IPCONFIG from DOS):
Did the virus exploit a vulnerability to infect the system:		Were Critical/Security Updates applied?
Yes No		Yes No N/A
If YES, which one?		If NO, why not?

SECTION 2: MACRO VIRUSES

Was NORMAL.DOT infected? Yes No NORMAL.DOT file date/time: _____ (prior to virus eradication)	Location of NORMAL.DOT. ___Server ___ Hard drive (If SERVER or Yes, page the ASSIST immediately at (202) 539-3808 and notify server Administrator.)
---	--

SECTION 3: FILE-BASED VIRUSES

Number of infected files: _____	If possible, attach list of infected files with file dates and times. (e.g., use DIR > LPT1: to list, then mark appropriate files.)
If the virus is a Startup Executable, clear the the Registry Run entries, either manually or with a tool.	

SECTION 4: BOOT SECTOR VIRUSES

Number of diskettes infected: _____ Number of systems infected: _____	If the system was infected, why did the user boot from diskette? _____
--	---

SECTION 5: E-MAIL INFECTIONS

If possible, print message (address list), attach, and answer the following questions.

How was the e-mail message received? DOE Outlook/Exchange Internet Mail	If Internet mail, indicate the ISP (e.g., HotMail, Yahoo, AOL):
Who was the sender? _____	Has the sender been notified of the virus? Yes No By whom (circle one)? User ViRT Gateway
Who else received it? _____ _____ _____	Have recipients outside of HQ been notified? Yes No By whom (circle one)? User ViRT Gateway Have recipients within org. been visited? Yes No
Post Offices with infected e-mail: _____	

SECTION 6: MEDIA INFECTIONS

Type of media: Diskette Zip Disk CD Number of diskettes/media infected: _____	Were infected media used in other DOE systems? Yes No If yes, user name: _____ Room : _____ Were they contacted? Yes No
Who provided the media? _____	Has the provider been notified of the virus? Yes No By whom (circle one)? User ViRT
Who else received or used the media? _____ _____	Have users been notified? Yes No By whom (circle one)? User ViRT

POTENTIAL QUESTIONS FOR MEDIA INFECTIONS:

Does anyone else use the system?	[] Yes [] No If yes, whom? _____
Have you recently received diskettes from anyone?	[] Yes [] No If yes, whom? _____
Have you recently given diskettes to anyone?	[] Yes [] No If yes, who? _____
Do you share diskettes between home and work?	[] Yes [] No
Is your home system protected against viruses?	[] Yes [] No Package? _____
Have you used other systems at DOE, Colleges, End User Center, etc..	[] Yes [] No Where? _____
Has AOSS Support Team or Hardware Tech. performed work on PC lately?	[] Yes [] No Who? _____ When? _____
Have you ever had a virus before?	[] Yes [] No When? _____

IMPACT

Was any data lost?	Yes	No	If yes, was the data recovered?	Yes	No
Was system operability lost?	Yes	No	If yes, was operability restored?	Yes	No
Did any data compromise occur?	Yes	No			

(If you answered Yes to any question, provide detail in Notes below.)

ViRT/AOSS Support Time to complete incident: _____

User/system productivity time lost: _____

FOLLOW-UP

For out-of-organization response, was AOSS Support contacted?	Yes	No	N/A
--	-----	----	-----

Name: _____

Phone #: _____

NOTES

Provide additional information here. It is important to describe how each media item (file, diskette, system) became infected. A complete history of the virus spread, from source to all affected parties within DOE, must be provided, including resolution of all system examinations. For simple encounters (virus detected immediately on protected system, no other DOE recipients, and no spread to other users), information in previous sections should be sufficient.

SUMMARY

The information on this Investigation Form must provide sufficient information to answer the following questions (where knowable):

- Where did the virus come from (if traceable)?
- How was the virus able to infect the system (i.e., what were the protection failures on the system and on any other defenses that the virus had to pass through)?
- What actions were taken to correct any protection failures?
- What steps were taken to eradicate the virus?
- What the impact on the user/system was?

If any additional information is needed to ensure that these questions are clearly addressed, please provide it in the Notes section above.

CERTIFICATION

I certify that the infected system is clean of viruses, that anti-virus software is installed, active, and current, and that any applicable security patches have been applied.

Name

Signature

Date